Journal of Research Administration
Society of Research Administrators International

INTRUSION DETECTION AND PREVENTION FRAMEWORK IN A HONEYPOT CLOUD NETWORK USING HIDDEN MARKOV MODEL

V. Jayalakshmi[1*], R. Ponnusamy[2]

[1*]Research Scholar, Department of Computer Science, Mother Teresa Women's University, Kodaikanal, TAMILNADU. shruthivasu07@gmail.com

[2]Professor & Dean, Dept. of Computer Science & Engineering, Chennai Institute of Technology, Kanchipuram, TAMLINADU. prof.r.ponnusamy@gmail.com

***Corresponding Author:** V. Jayalakshmi

*Research Scholar, Department of Computer Science, Mother Teresa Women's University, Kodaikanal, TAMILNADU. shruthivasu07@gmail.com

Abstract: With the fast expansion in the quantity of users, there is an ascent in issues connected with hardware failure, web hosting, space and memory allocation of data, which is straight forwardly or in a roundabout way prompting the deficiency of information. With the goal of offering types of assistance that are solid, quick and low in cost, we go to distributed computing rehearses. With a gigantic improvement in this innovation, steadily expanding chance of its security is being undermined by Honeypot. A method for redirecting vindictive traffic from frameworks is by utilizing Honeypot. An enormous methodology has given indications of progress in security of frameworks. Remembering the different legitimate issues one might look while sending Honeypot on third-party cloud vendor servers, the idea of Honeypot is carried out in a record sharing application which is conveyed on cloud server. This paper examines the detection attacks in a cloud-based environment as well as the utilization of Honeypot for its security, subsequently proposing a Intrusion detection framework design utilizing Hidden Markov Model Algorithm. This framework considers each stage utilized by ongoing intrusion and applies them to the Hidden Markov Model algorithm to figure out which intrusion is utilized in the audit data. This architecture diminishes overheads of intrusion agents and raises efficiency of the entire framework.

Keywords: Honeypot, Hidden Markov Chain, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), MD5.

1. INTRODUCTION

Intrusion Detection System (IDS), likewise referred to as the 'functionality of firewall' goes about as the critical component of framework security. It is utilized to recognize the exercises of the malicious in the LAN. A basic IDS contains the data set, design, identifier, counter measure, and data framework. IDS are ordered in view of the host-based and network-based IDS. The host-based IDS are related with the review logs and the information source framework calls. It additionally assists with investigating the doubles, secret phrase records and different exercises connected with the host. In network-based IDS buffer overflow attacks and denial of service attacks are analyzed. Furthermore, the attacks are distinguished by the host-based IDS and the network-based IDS. An Intrusion detection System is today perhaps of the best innovation in network security. Support vector machine (SVM), kernelized support vector machine (KSVM), Extreme learning machine (ELM), and kernelized Extreme learning machine (KELM) are a portion of the fundamental methods utilized in the intrusion detection system. A definitive objective of intrusion detection is to

foresee security violations in data frameworks. Information mining is utilized to keep up with and update the models in the interruption location framework by identifying extortion and shortcoming alert administration. An IDS safeguards a framework from split the difference, attack, and abuse. It assists with observing the network activity, system configuration vulnerabilities, data integrity analysis, weaknesses of framework designs and audits the network. It additionally tends to screen, recognize and produce the alert.

Honeypots are seen as a fruitful technique to follow developer lead and inspire the reasonability of security instruments. Honeypots are explicitly intended to deliberately connect with and deceive hackers as well as distinguish malicious activities performed over the WWW and can be considered a successful strategy to follow hacker behavior. Honeypots can be characterized as frameworks or resources which are utilized to trap, screen yet to likewise distinguish incorrect solicitations present inside a network. They shift in the communication gave to the attackers, from low association to medium and high, each type enjoys its benefits and weaknesses. Their aim is to dissect, comprehend, watch and track attacker's behavior to make frameworks that are secure as well as handle such traffic. It is a firmly observed computing resource that we need to be tested, attacked, or split the difference. "All the more definitively, it is a data framework resource whose worth lies in unapproved or illegal utilization of that resource."

Detecting Intrusion in Cloud Based Systems IDS are utilized to identify dangers and give greater security in the cloud environment. It protects the Distributed Denial of Service (DDOS) attack in the cloud framework. IDS stand as firewall security in which it shields the framework from different malicious attacks on the WWW. It is utilized to break in through the firewall security and it likewise attempts to keep the framework on the confided in side of safety. Moreover, the IDS is utilized to mechanize the checking process and it additionally creates reports to the station of the management. IDS centers the network traffic and suspicious action which enacts a alert to the network admin chairman to avoid the causes. Signature-based IDS screen the packets on the organization and identify the malware in an effective way. Interruption discovery network are like programming and equipment components that recognize abnormal exercises for further investigations. I has played an important role in grid security management. It is utilized to identify anonymous intrusions, known intrusions, and different sorts of risky occasions; aside from recognizing threats and attacks however here and there it gives bogus alerts. Grid frameworks support the security approaches for the information lattice and assist with prevent future attacks inside the Computing Environment. The IDS frameworks for service grid coordinate assets of node identification in the computing application. IDS can help the Cloud Management Platforms (CMPs) to offer secured services. Advantages of CMPs and a relative investigation of highlights given by major CMPs like OpenNebula, CloudStack, Eucalyptus and OpenStack were well implemented.

Impact of Intrusion on the Performance of Cloud Based Systems

The cloud computing IDS is utilized to coordinate information and conduct examination to identify intrusions. The computing environment is the objective for intruders to exploit. The intruders can utilize vindictive codes to attack the framework. IDS offers high and extra safety efforts for these sorts of environment by breaking down the configurations, network traffic, and attack conduct of the user. IDS can be prompted and conveyed in the grid and cloud computing environment to give firewall security. It likewise has the capacity to identify the attack in every hub in the cloud-based framework. It additionally alarms each hub in the computing environment and this correspondence makes an effect in the communication system.

Attacks are not appear able to host-based IDS. The IDS has utilized the two methodologies, for example, the performance approach and the data approach. The exhibition approach is utilized to contrast the client activities with the typical way of behaving. The data approach is utilized to see specific arrangements of activities which additionally address an assault. At last, IDS is utilized to

further develop energy effectiveness and security in the cloud-based environment assessed energy utilization of a virtualized server in a data centre.

Layers of Cloud

Like an onion, the Cloud has many layers. It is normally partitioned into 3 layers: 1. Infrastructure as a Service (IaaS) 2.Platform as a Service(PaaS) 3.Software as an Service (SaaS). Out of the three layers, SaaS is the top layer working off of both Paas and Iaas while Iaas is the underpinning of the entire structure. The Infrastructure as a Service (IaaS) layer is actual hardware and hence Honeypot manages this layer. The Cloud depends on actual physical hardware reasonable for Computing (eg. hubs, servers and so on). Information are put away in what are called data centres (otherwise called DC) which are worked by web hosting experts or network engineers.

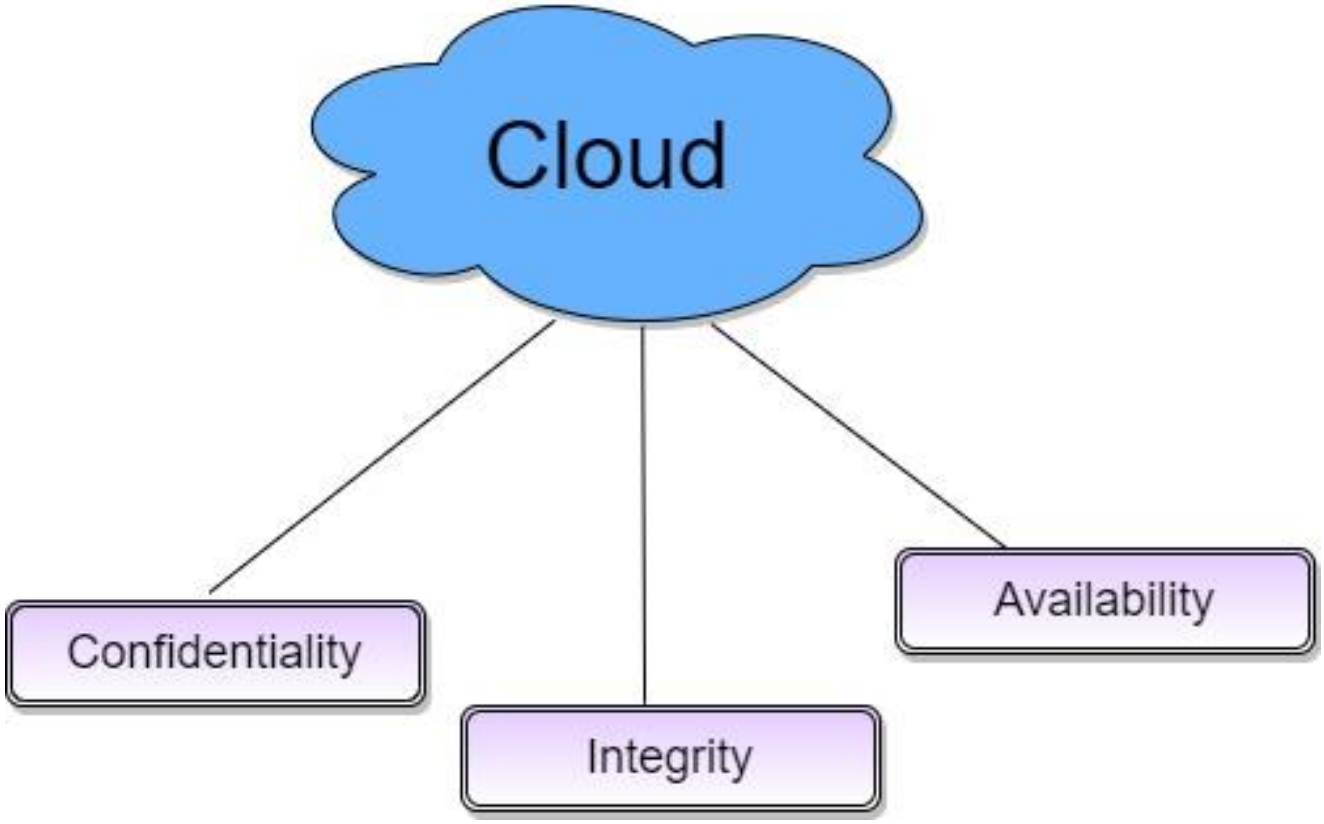

Fig 1: Cloud Security Threads

Types of Security Threats

Cloud computing faces many security threats. These threats are of various forms. Following are the threats recognized at universal level:

- Traffic Hijacking.
- Insecure Interface and APIs.
- Denial of Service.
- Malicious Insiders.

Cloud Honeypots

Cloud-based Honeypots provide the ability to investigate and look at attacks that hit conventional customers. Having them allows an expert to decipher the IP areas and malware being used into

security content that can guarantee a typical cloud environment. When those IP addresses have been recognized, they will then, at that point, lead a ping degree and helplessness result to find a weakness in the framework blueprint or weaknesses in programming that can be abused. It's prominent yet real; horrendous people seek after the most vulnerable centers the most frequently. There are potential gains of using a cloud build Honeypot considering a cloud system resembles standard Honeypots in that it should have the ability to conclude whether a cloud structure has been compromised or tries were made to do as such. Finally, they can basically sit and log all development coming into the cloud site; and considering the way that it's used for this specific explanation for all intents and purposes any activity should be managed as in a flash dubious. Honeypots can make risks more self-evident and go probably as an early ready system, which gives a cloud association a more proactive method for managing security using hidden markov chain model. Any relationship with either outside assets/regions or cloud organizations should send cloud-based Honeypots.

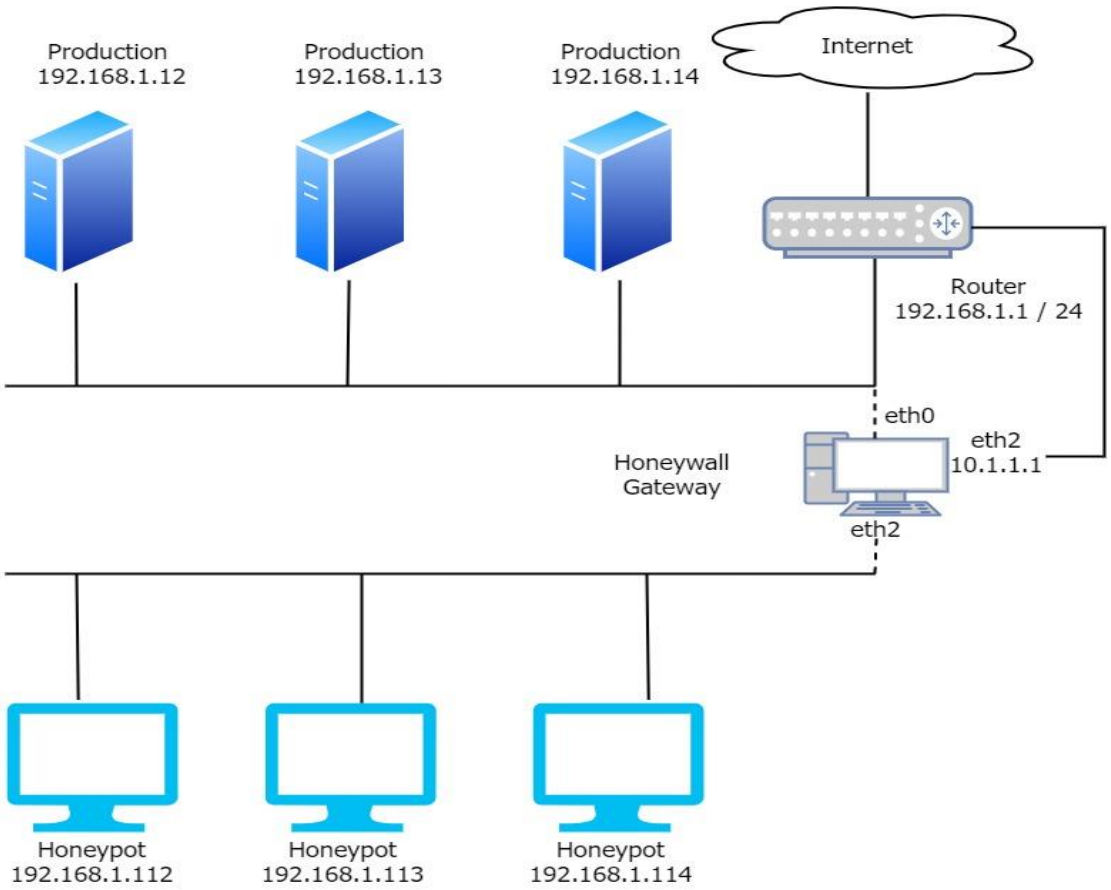

Fig 2: Functioning of Honeypot

A Honeypot is an identification and security gadget which is expected to be tried, attacked, or haggled. The sole goal is to allow the Honeypot to be viewed as like some other typical machine or framework by an unapproved element, introducing it as a snare. Their action can be followed without being thought while doing as such. It is utilized to recognize and respond, rather than making a balancing move, a region where it doesn't convey a lot of skill. Since Honeypots can't keep a particular interference or spread of contamination or worm, it simply accumulates information and recognizes attack plans. A Honeypot is a gadget to assemble affirmation or

information, and to get whatever amount of advancing as could sensibly be anticipated especially on the attack plans, programmer's explanation and motivations and the regularly used projects pushed by them. From every one of the information, we can find out about the programmer's ability especially their particular learning. Honeypots can be used to redirect malevolent software engineers from general systems to the Honeypot structure. It tends to be carried out in a cloud-based climate by either setting it before the firewall or after the firewall. Another way is to carry out it through an application which gives recognition as well as gives security to the records being shared through that application. This Application can later be transferred/sent on a server which can likewise go about as a cloud later. A cloud framework with Honeypot present at its base is definitely more safeguarded than the ones that don't contain it.

Types of Honeypots

Honeypots are divided mainly into two types:

1. Low interaction

2. high-interaction Honeypots.

a) Low- Interaction Honeypot: Low-interaction Honeypots practice restricted cooperation. This is on the grounds that the attacker movement is restricted to the degree of copying by the Honeypot. Low-cooperation Honeypot have a straightforward design and in this manner they are not difficult to send. They are significantly simpler on the upkeep side, offering minimum risk. Besides, the attacker is always unable to get to a operating system in order to infect remaining systems. The fundamental drawback of this sort of Honeypot is that restricted data is signed on the Honeypot database which likewise catches any unapproved action. "It is likewise more straightforward for an attacker to distinguish a low interaction Honeypot, regardless of how great the copying is, a talented attacker can ultimately recognize their presence.". Examples of low-interaction Honeypot incorporate Specter, Honeyd, and KFSensor.

b) High- Interaction Honeypot*:* High-interaction Honeypots are typically difficult in contrast with low interaction Honeypots, the explanation of their intricacy being: real time connection with programming and applications. Attackers are given real time frameworks and programming. Broad measures of data can be caught in this sort of Honeypot deployment and an open environment is give that catches every type of effort. This permits high-interaction answers for learn conduct we wouldn't anticipate.

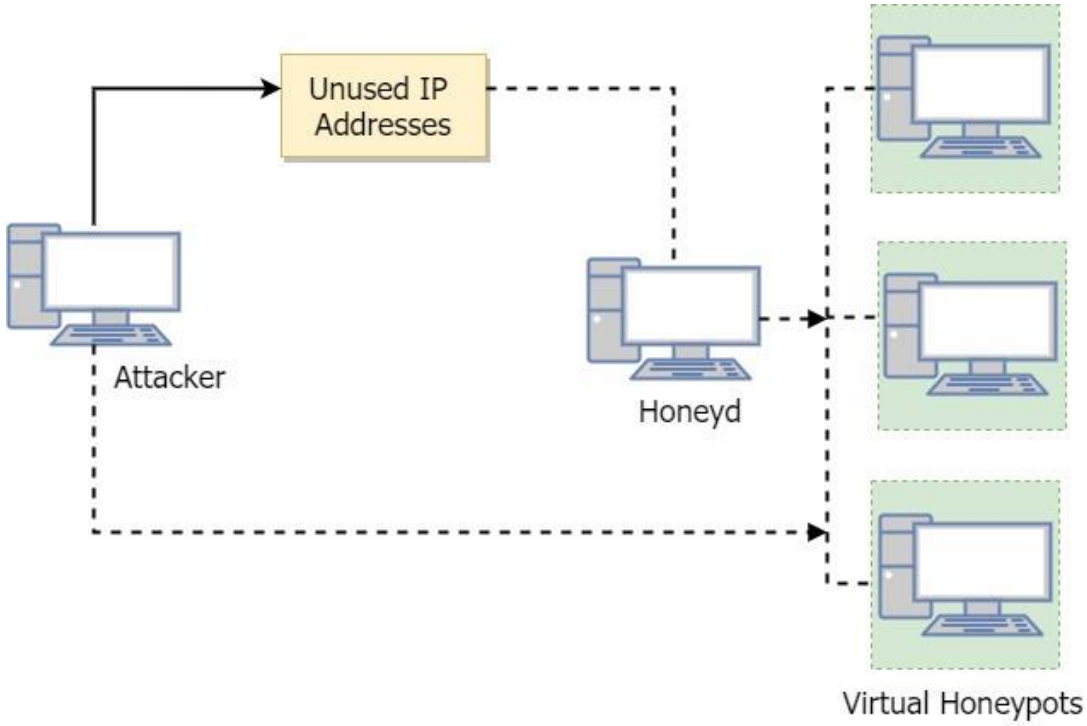

Fig 3: Honeyd Monitors

2. LITERATURE SURVEY

P. H. Yashwant et al examines about the Honeypot, which fills in as cutting edge security apparatus limiting the dangers from attack on IT and networks.A Honeypot is vital instrument for spotting network attacks [17]. Lofty sahi guaranteed extended degree of safety in the Cloud computing environment and a decrease in the threats to the Cloud climate, Honeypots connect with the assailant and gather information that can be examined to recover data in regards to the attacks. By zeroed in on the issue of Cloud data capacity. At the point when utilized by an association to utilize the organized IDPS and Honeypot, the system proposed is down to earth and the model is fruitful. A method for redirecting malignant traffic from frameworks is by utilizing Honeypot. A titanic procedure has given indications of progress in security of frameworks. Remembering the different lawful issues one might look while sending Honeypot on outsider cloud seller servers, the idea of Honeypot is carried out in a record sharing application which is conveyed on cloud server [26]. S. Ravji and M. Ali examines the location attacks in a cloud-based environment as well as the utilization of Honeypot for its security, subsequently proposing another strategy to do the same [19].

VinothKumar et.al proposed framework: Blockchain is to diminish the assault rate in view of its cloud. Be that as it may, the miner node in the Blockchain deals with the attacks, for example, phishing attacks, wallet attacks, word reference based attacks, co-opposition attacks. The Author profoundly manages planning and organization of a staggered confirmation system to safeguard blocks of records among the different local area of people groups on the cloud [23]. J S. KumarSharma and M. Manoria list out Machine learning algorithms such as Hidden Markov Model and Outrageous slope help calculation can be utilized for interruption location in light of CICIDS dataset. In light of dataset, calculations make classifiers of marks of particular attack. These prepared classifiers are tried against client information for interruption identification. Framework reports assault in network. XGBoost classifier gives higher precision contrasted with HMM classifier [22]. K. Zhang gives an exhaustive survey of the writing regarding the matter of the recognition and relief of wormhole attacks in wireless sensor networks. The current overviews are

likewise investigated to track down holes in the literature. Several existing schemes in view of various techniques are likewise assessed basically as far as throughput, recognition rate, low energy utilization, bundle conveyance proportion, and start to finish delay. As man-made consciousness and AI have gigantic potential for the proficient administration of sensor organizations, this paper gives artificial intelligence and ML-based plans as ideal answers for the recognized cutting edge issues in wormhole attack detection [1].

M. Shukla proposed Particle Swarm Optimization (PSO) is used to improve the features of planning framework data and a short time later totally associated Deep Neural Network (DNN) is used to set up a Network Intrusion Detection System (NIDS) through coordinated learning. Significant brain framework models are arranged using NSL-KDD dataset that rout obstructions of KDD Cup2009 interference acknowledgment datasets which has been consistently used previously. With NSL-KDD datasets, significant brain frameworks with particle swarm improvement are exhibited to be strong to the extent that precision and recognition rate. The best basic attacks in MANET are wormhole assault and jellyfish attack. The composing needs inside the techniques that could interminable inventory of these attacks at the same time. In this assessment, a planned system that is prepared for stumble on both wormhole and jellyfish attack the use of unclear limits [10]. C.-L. Chen et.al proposed a framework, network intrusion detection (NID) framework might be furnished with AI calculations to accomplish better precision and quicker recognition speed. Most of interruption avoidance frameworks utilize the discovery techniques which incorporate Mark based, Measurable irregularity based and Honey pot based. Utilizing these location techniques, the malware is recognized, and afterward further moves are initiated to obstruct the malware. IPS strategies vary by the way they check the information streams to distinguish a danger or interruption. Information catch and information control are involved by the examination local area to concentrate on issues in network security, for example, Web worms, spam control, and Denial of Service (DoS) attacks. In this paper, we will zero in on avoidance from the different kinds of attack [28].

The proposed technique joined the superior teaching-learning-based optimisation (ITLBO) algorithm, improved parallel JAYA (IPJAYA) algorithm, and backing vector machine. ITLBO with managed machine learning (ML) procedure was utilized for highlight subset determination (FSS). The determination of the least number of features without causing an impact on the outcome exactness in FSS is a multi-objective enhancement issue. This work proposes ITLBO as a FSS component, and its calculation explicit, parameter less idea (no boundary tuning is expected during advancement) was investigated. IPJAYA in this study was utilized to refresh the C and gamma boundaries of the support vector machine (SVM). A few investigations were performed on the noticeable interruption ML dataset, where significant improvements were seen with the recommended [23]. M. Aljanabiet.al proposed ITLBO-IPJAYA-SVM algorithm contrasted and the old style TLBO and JAYA algorithms [16].M. Bandgar portrayed novel approach using Hidden Markov Models (HMM) to detect Internet attacks [15]. V. Bajaj et.al depicts an intrusion detection system for identification of signature based attack. These attack marks envelop explicit traffic or movement that depends on known meddling action [20]. H. Banafar et al performed single and different HMM model for source division both on IP and port data of source and objective. This approach decreased the misleading positive rate and we made this sort of source partition as our essential step for building HMM [27]. W. K. Zegeye et.al proposes a multi-stage intrusion detection system architecture utilizing Hidden Markov Model Algorithm. This framework considers each stage utilized by ongoing interruptions and applies them to the Hidden Markov Model algorithm to figure out which intrusion is utilized in the audit data. This architecture diminishes overheads of intrusion agents and raises effectiveness of the entire framework [14].

D. H. Lee proposed the use of HMM to IDS usually alluded as the scourge of dimensionality. It factors a gigantic issue of monstrous dimensionality to a discrete arrangement of reasonable and dependable components. The multi-layer approach can be extended past 2 layers to catch multi-stage assaults over longer ranges of time. A pyramid of HMMs can determine different computerized occasions and marks across conventions and stages to significant data where lower l layers identify discrete events (such as network scan) and higher layers new states which are the consequence of multi-stage occasions of the lower layers. The ideas of this original methodology have been grown yet the maximum capacity has not been illustrated [13]. K. Venkatachalapathy and VinothKumar. J proposed research work identifies the various attacks and pay attention to eliminate them by introducing a novel Virtual Machine (VM) placement policy through Markovian chain with security, load balancing and energy consumption as optimization objectives [11].

S. Al-Ahmadi et.al and K. Zhang proposes to the methodology of Multi-layer Encryption wireless sensor techniques in cloud computing accordingly upgrading the security boundaries concerning delicate information Consequently with layer ways Encryption strategy the information in cloud server can be made more gotten with better protection. Resultant both cloud application and patient information improved security. As per this encryption strategy on the off chance that information proprietor's approval isn't allowed then the clients are confined from the information access. The cloud applications that are basic can be profited from the above proposed calculation which professes to be straightforward and proficient. The numerical model of information disguising for giving misleading shift focus over to delicate information prior to moving information to cloud and MAC address subordinate AES strategy for moving non-delicate information and cleaned information is proposed in the paper [21].V. K. J and K. Venkatachalapathy proposed a multi-level security technique is suggested in cloud computing. Accordingly ad improvising the security boundary in regards to clinical delicate information. Accordingly, the AES-SHA blend of calculation and solid cyclic watermarking model used to send the information to the cloud chief. It offers better security execution, enhances the getting sorted out of medical data and guarantees secrecy [9].

B. Devanathan proposed framework likewise gives a safe data sharing plan for the powerful gathering in a cloud environment. Any client in the cloud can impart the information to different clients by the utilization of a group signature. The group signature is produced with the assistance of end-user accreditations for secure information sharing. A gathering part will send their certification to the gathering director. In the wake of checking the client accreditation, the gathering chief will give the gathering mark to the gathering part for getting to and sharing information in the cloud. In the proposed framework, the expense of calculation isn't subject to the quantity of the repudiated client [4]. K. M. A. Alheeti et.al tackle a few existing techniques have confronted issues like low classification accuracy, high false positive rates, and low true positive rates. To overcome above issues, a detection system in light of Help Vector Machine (SVM) is proposed. In SVM, SVM classifier is used for network information grouping into ordinary and unusual ways of behaving. The Cloud Interruption Location Dataset is utilized to test the viability of the proposed framework. The exploratory outcomes show which the proposed framework can recognize abnormal behaviours with high accuracy [3].

3. PROPOSED TECHNIQUE

In the proposed structure, Honeypots can likewise be perceived by taking a gander at the manners in which cloud frameworks are being utilized in relationship with IDSs to prevent, recognize and help answer attacks. For sure, Honeypots are progressively finding their place close by network and host-based IDS. Honeypots can prevent attacks in more than one way. The first is by dialing back or halting robotized attacks, like worms or auto rooters. These are assaults that arbitrarily examine a whole networks searching for vulnerable nodes in network. (Honeypots utilize an assortment of TCP stunts to place an assailant in a "brief delay.") The subsequent way is by dissuading human attacks. Here Honeypots plan to divert attacker, causing him to dedicate thoughtfulness regarding activities that inflict neither kind of damage nor misfortune while giving an organization time to answer and freeze the attack.

A **Markov cycle** is a stochastic process(irregular cycle) in which the likelihood dissemination of the present state is restrictively free of the way of past state , a trademark called the Markov property.

Markov Property: The state of the system at time t+1 relies just upon the state of the system at time t Hidden Markov Models (HMMs)) are utilized for circumstances in which: The information comprises of a grouping of perceptions. The perceptions depend (probabilistically) on the internal state of a dynamical system. The genuine state of the system is unknown (i.e., it is a covered up or inactive variable).

This gives the security of two kinds:

a. Inside the cloud(within cloud environment)

b. Outside the cloud (outside cloud environment)

This model gives security in two stages:

Stage 1: In first move toward quite a while validation of user. If it is valid user then stepping in it into cloud environment any other way it can't enter in cloud environment.

Stage 2: Assuming user is substantial client enter in the cloud climate and send and recover information to Data Centre. After that following strategy is finished:

Philosophy

1. Create cloud reproduction climate comprising of dynamic number of clients and data centres.
2. As soon as the cloud is laid out the source can send packets to the data centres.
3. Now instate the HMM with specific arguments at server or agent level of the cloud.
4. The number of states in the model will relies upon the clients in the cloud.
5. As soon as the packets begin sending from client to data centres. HMMs begins computing the likelihood of every one of the packet in the transition state.
6. If the likelihood of packets surpasses threshold value then a detector is begun to detect the intrusion in the packet.

Verification

Message Verification is the strategy to confirm that the got message come from supposed source and have not modified. We need to confirm the identity of who we are transferring with. We need to guarantee that what they sent is what we got (integrity). We would rather not permit unapproved registrations.

MD5

MD5 algorithm was developed by Professor Ronald L. Rivest in 1991. According to RFC 1321, "MD5 message digest algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest"of the input …The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA".

Prevention of Intrusion

This study examines the Hidden Markov Model which can be used to detect and prevent intrusion in the cloud. This model can reduce false alarm in the cloud environment. Accuracy, false alarm rate, and detection rate are also used to evaluate the performance of the intrusion detection system. The proposed IDS using the feature selection method to improve detection accuracy and efficiency. IDS technique based on feature selection in their article. Using rough set theory, they reduced the number of features to half of the original set. They demonstrated in their work that feature selection can reduce system complexity while improving system performance. The HMM (Hidden Markov Model) can be deployed as a kind of topology and statistical parameters. It is probable for converting the action of a user into the appropriate dataset and trains it. Then the trained data are adopted for further prediction.

HMM is a generative model that can model data which is sequential in nature. It is used to model data where the Assumption *Markav property:* Consider a system with N states and at discrete time intervals, there is transition among states. Let these instances be t, t = 1, 2, 3, · · · .Any process is Markovian if the conditional probability of future states, given the present state and past states, depend only upon the present state

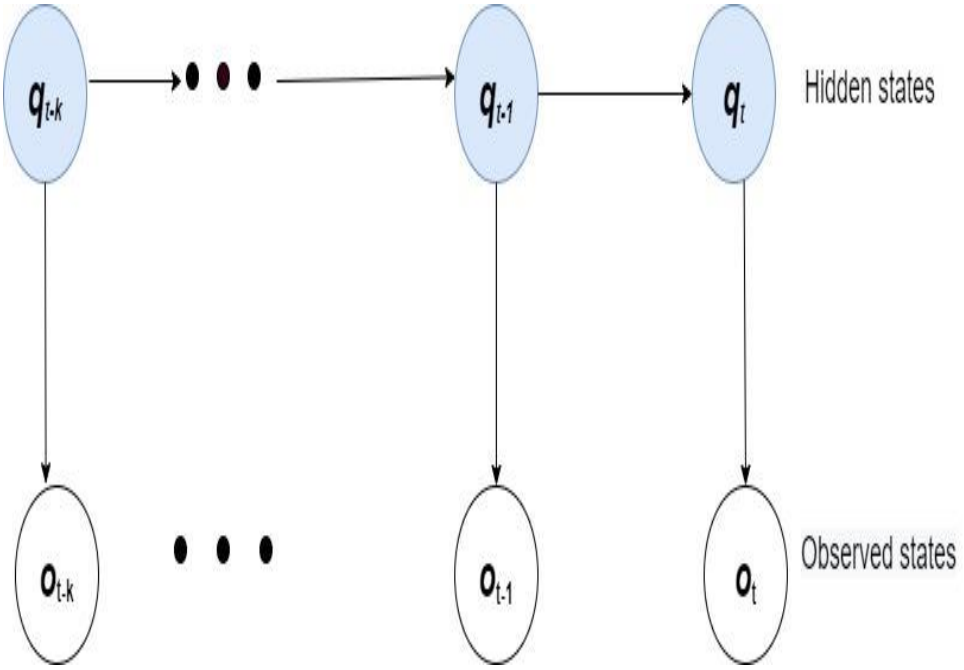

Fig 4: Hidden Markov Model

The steps followed in the proposed system are:

1) Build a simulation environment for the cloud which involves an active quantity of data centers and users.

2) The transmitter can transmit packets to data center when establishing the cloud environment.

3) Choose the dataset on which testing and training of detecting intrusions is performed.

4) Train the dataset for input after finishing training it will create numerous rules.

5) After that, Hidden Markov Model is started with definite parameters at the broker cloud level or server.

6) Quantity of states involved in the model will rely on the clients in the cloud.

7) After that, the client initiates packet distribution to the data center, then the hidden markov model initiates computing the probability of every packet in the state of transition. At the same time, if any packet probability exceeds the already defined value for the threshold; then a system for rule is developed based on the feature values of the intrusion detection system dataset.

8) And then finally based on the value for the threshold, remove the packets.

A hidden markov model involves 5 tuples:

1. S represents the number of states present in the model A {A1, A2, A3, A4, A5…..}

2. represents the number of symbols in the observation B {B1, B2, B3, B4, B5….}

3. T denotes state probabilities in the transition

4. D represents each state's distribution

5. Π denotes the initial distribution of the state.

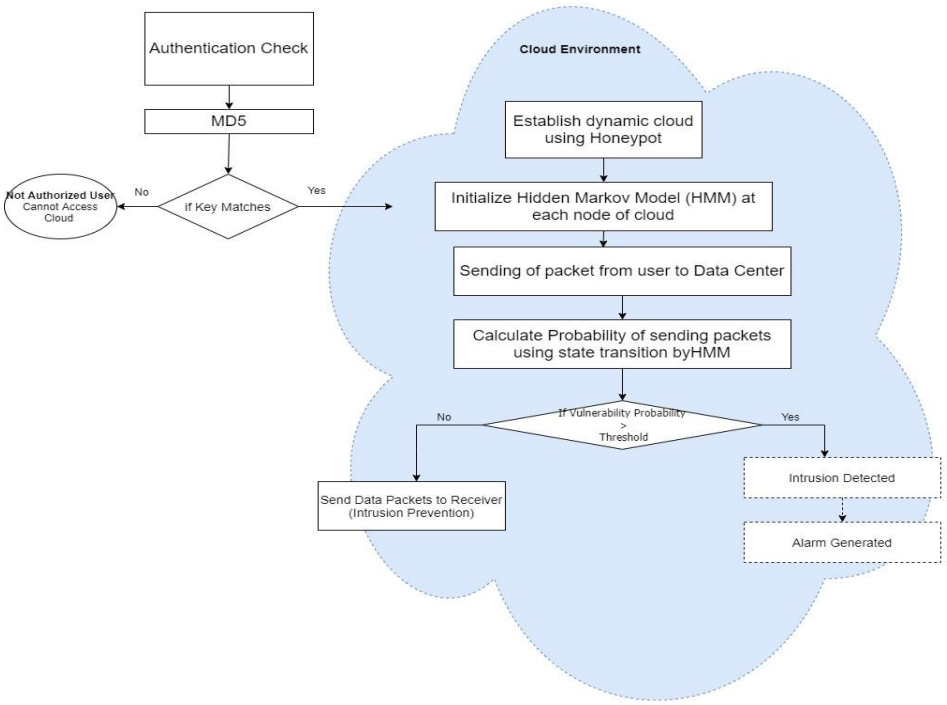

Fig 5: The Proposed Architecture - Hidden Markov Model in Honeypot Cloud

The prevention of the intrusion in the cloud environment can be prevented by increasing average threshold of the transition states of the packets of the packets 'pkt'.

1. The initial transition probability from one state Q1 to another state Q2 at a particular instance of time t+1 depends on the state at time t according to the assumpt ---------- (1) **ιij =p(qt+1 = sj | qt = si)**

2. The probabilities of the transition of the states is independent of the actual time where the transition takes place according to the assumption of stationarity i.e ---------- (2)

p(qt+1 = sj | qt1 = si) = p(qt2+1 = sj | qt2 = si)

3. Lets 'n' is the number of packets 'pkt' send at a particular transition at a particular instance of time.

4. Compute each step of the transition the state which is generally plausible for the observation, probability of state transition δt can be calculated utilizing viterbi calculation.

5. After each step of the transition, work out the general probability of the packet to be sent at each step Q.

6.The average probability can be computed using ---------- (3)

$\delta avg=(\Sigma\ k=1T\delta k(i))/T$ ---------- (4)

$\delta avg=(\Sigma\ k=1T\delta k(i))/T+1$

7. The condition is checked at each node of the cloud means the next state and the previous state of the transition i.e. if the average probability is less than the next average threshold value then the packets is transferred from the next other transition state.

The Viterbi algorithm seen as finding the shortest route through a graph is:

Input: $Z=z_1, z2, ..., zn$ the input observed sequence

Initialization:

$k=1$ time index

$S(c_1)=c_1$

$L(c_1)=0$ this is a variable that accumulate the lengths, the initial length is 0

Recursion:

For all transitions $t_k=(c_k,c_{k+1})$

Compute: $L(c_k,c_{k+1}) = L(c_k) + I[t_k = (c_k,c_{k+1})]$ among all c_k.

Find $L(c_{k+1}) = \min L(c_k,c_{k+1})$

For each c_{k+1}

Store $L(c_{k+1})$ and the corresponding survivor $S(c_{k+1})$.

$k=k+1$

Repeat until $k=n$

RESULTS AND DISCUSSIONS:

The existing approaches such as Modified zone based intrusion detection system (MZBIDS) and energy-aware resource provisioning algorithm for Real-Time Cloud services (EA-ICA)] are studied and analyzed with proposed HMM technique which is based on storage and search optimization. The Proposed HMM calculates the QoS performance, such as the end-to-end delay, the network lifetime, the packet delivery ratio, and the throughput. In addition, the area under the curve (AUC) is plotted for binary classification problems. AUC is the measure of a router's ability to distinguish between routes and summarize the score chart.

AUC Chart: An accurate system will detect the chart's intrusion, showing different points and stating the entire false positive and true positive rate (fig 6). In addition, the system also provides the accuracy of the proposed algorithm stated on the chart. With this data, the number of packets containing intrusion attacks is found. To describe the efficiency established by proposed HMM methods', fine-tuned accuracy is evaluated based on the following action to achieve an accurate result.

Detection rate (DR) - Ratio between numbers of anomaly correctly classified by the total number of anomaly in the database.

Error rate(ER) - Ratio between number of anomaly (normal) incorrectly classified and total number of anomaly (normal).

True positive (TP) - classifying normal class as normal class.

True negative (TN) - classifying anomaly class as anomaly class.

False positive (FP) - classifying normal class as an anomaly class.

False negative (FN) - classifying anomaly class as a normal class.

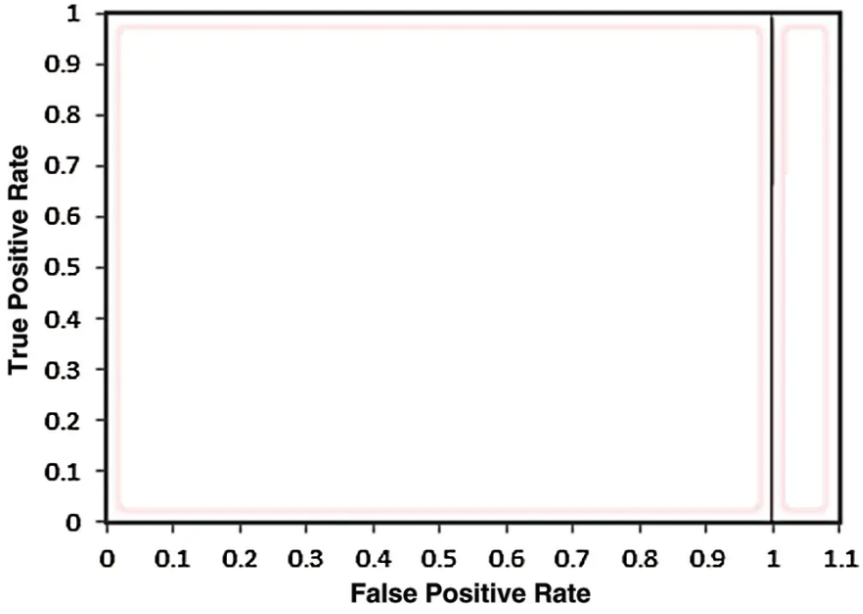

Fig 6: AUC Chart

Fig. 7 shows that accuracy is surveyed utilizing Eq. (5) for capacity and route sustentation, utilizing the proposed HMM. Involving the current techniques MZBIDS and EA-ICA in Tab.1, the proposed HMM viability is around 97.76%. Moreover, an exactness of almost 97% was accomplished by our proposed HMM.

$$\text{Accuracy} = \frac{\text{True Negative} + \text{True Positive}}{\text{True Negative} + \text{True Positive} + \text{False Negative} + \text{False Positive}} \quad \text{---------- (5)}$$

Node's Counts	MZBIDS	EA-ICA	Proposed HMM
10	87.67	95.65	97.933
20	83.98	94.76	97.9
30	83.1	93.59	97.857
40	82.78	93.59	97.833
50	82.56	92.84	97.79
60	81.75	92.45	97.765

Tab. 1: Accuracy Comparison Table

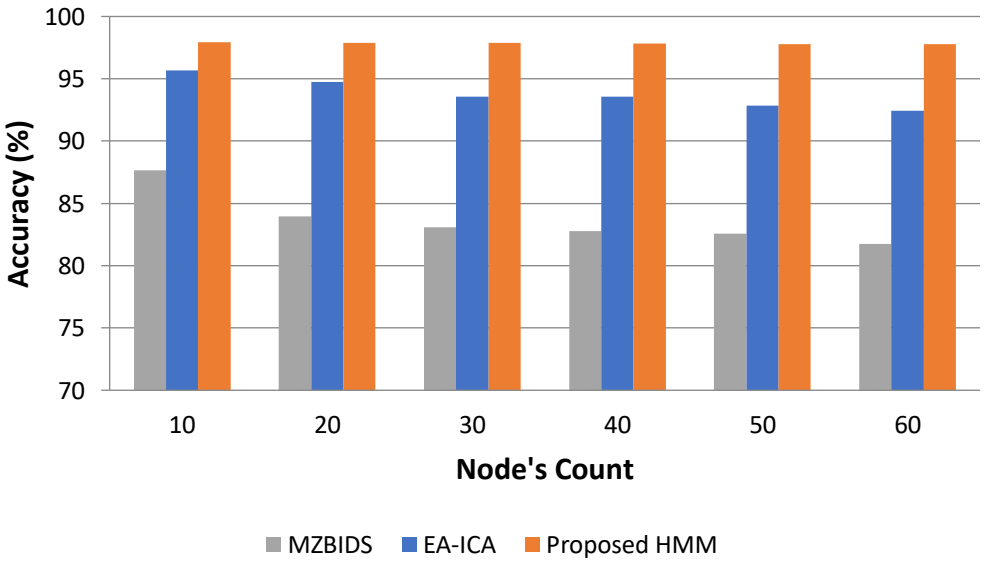

Fig 7: Accuracy comparison chart

Tab. 2 demonstrates that the proposed HMM technique can accomplish a high packet delivery ratio. The assessed measures show that the current MZBIDS acquires 92% in bundle conveyance proportion, while proposed HMM gets 97% in packet delivery ratio. Besides, a high PDR worth of 97.856% was gotten by the proposed technique, which is more remarkable than different strategies (Fig. 8).Packet is measured using Eq. (6):

$$P = \frac{\text{Total no of participated data packe}}{\text{Total no of transmitted data packets}} \times 100 \quad \text{---------- (6)}$$

Node's Counts	MZBIDS	EA-ICA	Proposed HMM
10	87.56	94.87	97.856
20	83.98	93.93	97.856
30	87.75	93.54	97.57
40	85.83	94	96.361
50	84.67	95.5	94.68
60	83.87	92.56	93.489

Tab. 2: Packet Delivery Ratio Comparison Table

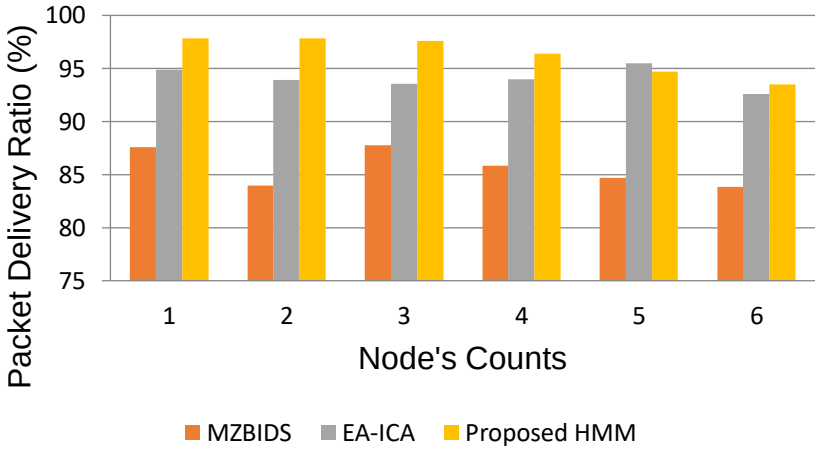

Fig 8: Packet Delivery Ratio comparison chart

Tab. 3 shows the throughput worth of the proposed HMM (Fig. 9). Throughputs of roughly 30 and 43 kbps are accomplished through existing methodologies, like MZBIDS and EA-ICA. The productivity of the proposed CLAID is additionally higher than the throughput execution of almost 121 kbps.

Node's Counts	MZBIDS	EA-ICA	Proposed HMM
10	10	10	16.416
20	15	17	19.426
30	18	21	112.416
40	23	27	116.433
50	26	34	119.426
60	30	43	121.333

Tab. 3: Throughput Comparison Table

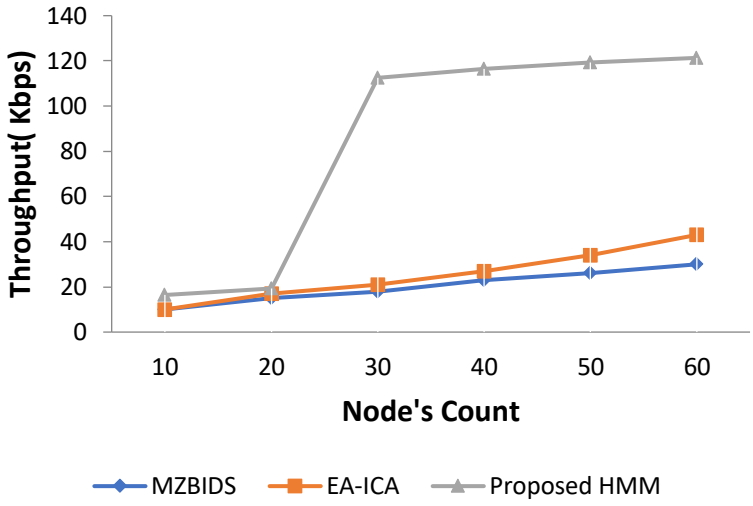

Fig 9: Throughput Comparison Chart

Fig.10 and Tab.4 depict the network lifetime for some nodes and the testing with dominating methodologies. While sending messages across 60 nodes, the current MZBIDS and EA-ICA have network lifetimes of 220 and 350 s, however the proposed HMM technique's greatest network lifetime 627.133 s. The postponement is estimated to distinguish the time expected to arrive at the objective of the transmitted data. The proportion of time consumed for receiving packets to the time consumed by the transmitted packets is estimated utilizing Eq. (7).

$$\text{End-to-end delay} = \frac{\text{Time Duration (Received data}}{\text{Time Duration (Transmitted data packets)}} \quad \text{---------- (7)}$$

End-to-end delay points of the proposed HMM method and contrasts the value and those of existing methods. Here, MZBIDS and EA-ICA get postpone upsides of around 59 and 43 s, individually. The proposed HMM strategy likewise gets a postpone worth of 14 ms. In correlation, the proposed HMM gets a lower delay points of 0.6 s while transmitting 10 nodes.

Node's Counts	MZBIDS	EA-ICA	Proposed HMM
10	98	110	127.133
20	115	140	277.324
30	140	186	397.199
40	167	230	507.199
50	198	267	557.613
60	220	350	627.133

Tab. 4: Network Lifetime Comparison Table

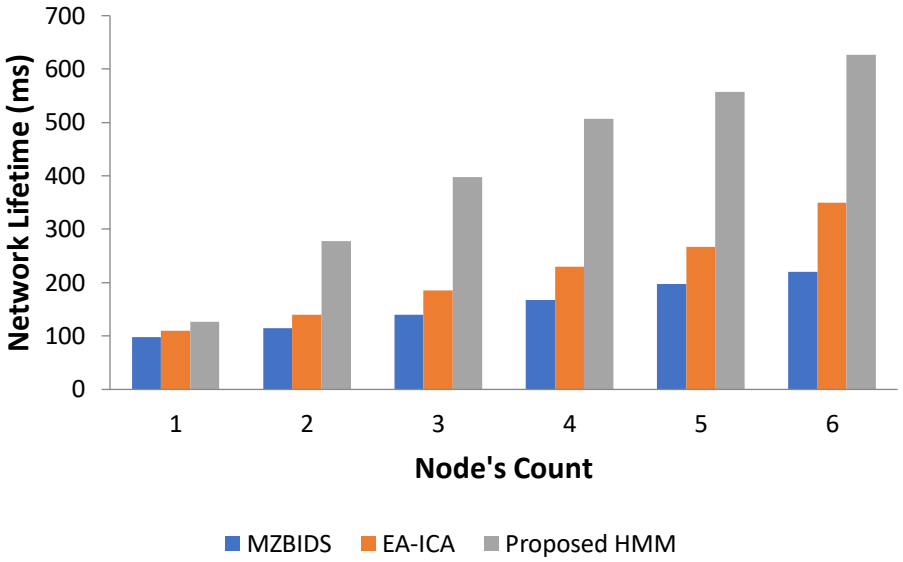

Fig 10: Network Lifetime Comparison Chart

4. CONCLUSION

This study examines various techniques used in the intrusion detection of the cloud environment. The study found that the Hidden Markov Model can be used to detect and prevent intrusion in the cloud. It can be used as an alternative option to incorporate the detection and prevention technique into cloud-based environment. In this study, the HMM (Hidden Markov Model) can be deployed as a kind of topology and statistical parameters. It is probable for converting the action of the user into an appropriate dataset and train it. Then the trained data are adopted for further prediction.

5. REFERENCE

1. K. Zhang, “A wormhole attack detection method for tactical wireless sensor networks,” PeerJ Comput. Sci., vol. 9, p. e1449, 2023.
2. Dhara Buch and D. Jinwala, “Prevention of Wormhole Attack in Wireless Sensor Network,” Int. J. Netw. Secur. Its Appl., vol. 3, no. 5, pp. 85–98, 2011.
3. K. M. A. Alheeti, A. A. A. Lateef, A. Alzahrani, A. Imran, and D. Al Dosary, “Cloud Intrusion Detection System Based on SVM,” Int. J. Interact. Mob. Technol., vol. 17, no. 11, pp. 101–114, 2023.
4. B. Devanathan, “A Novel underweight immutable biometric authentication for secured data transfer over the cloud Environment,” Mathya Bharthi ,vol. 83, no. 1, pp. 11–30,2023.
5. J. Vinothkumar and A. Karunamurthy, “ Recent Advancements in Artificial Intelligence Technology : Trends and Implications ,” Quing: International Journal of MultidisciplinaryScientific Research and Development vol. 02, no. 01, pp. 1–11, 2023.
6. V. K. J. K. Venkatachalapathy, “A Security System for Electronic Medical Records using Three Phase Efficiency Model on Cloud,” vol. 29, no. 7, pp. 4844–4860, 2020.
7. J. Vinothkumar and L. Parthasarathy, “A Two-Level Authentication Approach for Securing Data in Cloud,” pp. 1–11, 2022
8. P. Narwal, D. Kumar, S. N. Singh, and P. Tewari, “Stochastic Intrusion Detection Game-Based Arrangement Using Controlled Markov Chain for Prevention of DoS and DDoS Attacks in Cloud,” J. Inf. Technol. Res., vol. 14, no. 4, pp. 45–57, 2021.

9. V. K. J and K. Venkatachalapathy, “Secure Transfer of Medical data to the cloud using cyclic watermarking and Encryption Technique”, Solid State Technology” vol.63 no.5, pp. 37–47, 2020.
10. M. Shukla, B. K. Joshi, and U. Singh, “Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET,” Wirel. Pers. Commun., vol. 121, no. 1, pp. 503–526, 2021.
11. Vinothkumar. J and K. Venkatachalapathy, “Protection Based Virtualization Using Virtual Machine Placement Policy on Secured Medical Cloud,” Adalya J., vol. 9, no. 4, pp. 151–166, 2020.
12. P. S. Negi, A. Garg, and R. Lal, “Network for Cloud Security,” 2020 10th Int. Conf. Cloud Comput. Data Sci. Eng., pp. 129–132, 2020.
13. W. K. Zegeye, R. A. Dean, and F. Moazzami, “Multi-Layer Hidden Markov Model Based Intrusion Detection System,” Mach. Learn. Knowl. Extr., vol. 1, no. 1, pp. 265–286, 2019.
14. D. H. Lee, D. Y. Kim, and J. Il Jung, “Multi-stage intrusion detection system using hidden Markov model algorithm,” Proc. Int. Conf. Inf. Sci. Secur. ICISS 2008, pp. 72–77, 2008.
15. M. Bandgar, “Intrusion Detection System using Hidden Markov Model (HMM),” IOSR J. Comput. Eng., vol. 10, no. 3, pp. 66–70, 2013.
16. M. Aljanabi, M. A. Ismail, and V. Mezhuyev, “Improved TLBO-JAYA Algorithm for Subset Feature Selection and Parameter Optimisation in Intrusion Detection System,” Complexity, vol. 2020.
17. P. H. Yashwant, P. A. Sanjay, and S. S. Shekhanur, “Buckler: Intrusion Detection and Prevention using Honeypot,” Int. J. Res. Eng. Sci. Manag., vol. 2, no. 1, pp. 2–5, 2019.
18. S. Thapar, A. Purohit, B. Kanwer, A. Jaiman, A. Mounika, and V. S. Madhumala, “An Approach to Detect Wormhole Attack in Mobile Ad Hoc Networks Using Direct Trust Based Detection Approach,” Int. J. Intell. Syst. Appl. Eng., vol. 11, no. 6s, pp. 276–283, 2023.
19. S. Ravji and M. Ali, “Integrated Intrusion Detection and Prevention System with Honeypot in Cloud Computing,” Proc. - 2018 Int. Conf. Comput. Electron. Commun. Eng. iCCECE 2018, no. 05, pp. 95–100, 2018.
20. V. Bajaj and N. Parmar, “Anomaly Attack Detection of an Intrusion Detection System with Deep Learning Approach,” International Research Journal of Modernization in Engineering Technology and Science, vol. 02, no. 02, pp. 1222–1228, 2022.
21. S. Al-Ahmadi, W. Aliady, and A. Alrashedy, “An Efficient Wormhole Attack Detection Method in Wireless Sensor Networks,” Proc. - 26th Int. Conf. Circuits, Syst. Commun. Comput. CSCC 2022, pp. 240–249, 2022.
22. S. KumarSharma and M. Manoria, “Intrusion Detection using Hidden Markov Model,” Int. J. Comput. Appl., vol. 115, no. 4, pp. 35–38, 2015.
23. V. K. J, “A Multi-Level Authentication approach to protect medical records using Blockchain Technology”, International Journal of All Research Education and Scientific Methods (IJARESM), vol. 9, no. 4, pp. 746–756, 2021.
24. Z. Qin, N. Li, D. F. Zhang, and N. Z. Bian, “Improvement of protocol anomaly detection based on Markov Chain and its application,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 3759 LNCS, no. 60273070, pp. 387–396, 2005.
25. U. Khan et al., “Intelligent Detection System Enabled Attack Probability Using Markov Chain in Aerial Networks,” Wirel. Commun. Mob. Comput., vol. 2021.
26. Lofty sahi, “Honeypot: A Security Tool in Intrusion Detection,” Int. J. Adv. Eng. Manag. Sci., vol. 2, no. 5, pp. 311–316, 2016.
27. H. Banafar and S. Sharma, “Intrusion Detection and Prevention System for Cloud Simulation Environment using Hidden Markov Model and MD5,” Int. J. Comput. Appl., vol. 90, no. 19, pp. 6–11, 2014.
28. C.-L. Chen and J.-M. Chen, “Use of MARKOV Chain for Early Detecting DDoS Attacks,” Int. J. Netw. Secur. Its Appl., vol. 13, no. 04, pp. 01–11, 2021.

29. B. S and S. K, “Evaluation of Network Intrusion Detection Using Markov Chain,” Int. J. Cybern. Informatics, vol. 3, no. 2, pp. 11–20, 2014.
30. B. Deep and A. Jain, “Prevention and Detection of Intrusion in Cloud Using Hidden Markov Model,” Int. J. Res. -GRANTHAALAYAH, vol. 11, no. 2, pp. 40–46, 2023.