INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

ONLINE BANKING FOR MULTILEVEL AUTHENTICATION SYSTEM USING HIERARCHICAL INTRUSION DETECTION

Dr. S.Chand Basha, Principal
Global Institute Of Management , Ibrahimpatnam, Hyderabad.
Email : chandbasha.ong@gmail.com

ABSTRACT

Cyber-attacks are becoming more sophisticated and thereby presenting increasing challenges in accurately detecting intrusions. Failure to prevent the intrusions could degrade the credibility of security services, e.g. data confidentiality, integrity, and availability. Numerous intrusion detection methods have been proposed in the literature to tackle computer security threats, which can be broadly classified into Signature-based Intrusion Detection Systems (SIDS) and Anomaly-based Intrusion Detection Systems (AIDS). In this initially user will check client computer attacks by using phishing and Trojans techniques. By using banking services the network traffic is applied. If there are any attacks obtained then pharming, DNS spoofing and network interception techniques are applied. With the help of SSL communication network traffic is provided. Intrusion detection system will detect attacks. In this initially user will check client computer attacks by using phishing and Trojans techniques. By using banking services the network traffic is applied. If there are any attacks obtained then DNS spoofing and network interception techniques are applied. With the help of SSL communication network traffic is provided. Intrusion detection system will detect attacks. From banking website data will be transferred. At last online banking systems provides data and reduce errors. From banking website data will be transferred. At last online banking systems provides data and reduce errors. From results it can observe that multilevel authentication system using hierarchical intrusion detection architecture for online banking will improve accuracy, precision, F1-Score, security and reduce the attacks and time duration to perform the entire operation.

KEY WORDS: Cyber-Attacks, Accuracy, Precision, F1-Score, Security, Attacks, Time Duration, Multilevel Authentication System, Online banking, Hierarchical Intrusion Detection.

I.INTRODUCTION

With the rapid growth of Internet, computer attacks and intrusions are increasing and can cause financial loss to an organization or an individual. The number of malicious applications targeting internet banking transactions has increased severely in recent years [1]. This represents a challenge

ISSN: 2057-5688

not only to the customers who use such facilities, but also to the banking institutions which offer them. Detection of intrusions and attacks is an important issue during internet banking and e-commerce transactions. Intrusion Detection Systems have been proposed as an efficient solution to protect online financial systems against intrusions andattacks.

The evolution of malicious software (malware) poses a critical challenge to the design of intrusion detection systems (IDS) [2]. Malicious attacks have become more sophisticated and the foremost challenge is to identify unknown and obfuscated malware, as the malware authors use different evasion techniques for information concealing preventing detection by an IDS. In addition, there has been an increase in security threats such as zero-day attacks designed to target internet users. Therefore, computer security has become essential as the use of information technology has become part of our daily lives. As a result, various countries such as Australia and the US have been significantly impacted by the zero-day attacks.

Cyber security is becoming important for everybody. With the increase in cyber-attacks, our data is at risk, our systems are vulnerable to these attacks and our privacy does not exist. To protect our systems and ourselves from such attacks, there are many cyber security tools available. Among these tools, the Intrusion Detection System is an important tool that protects our data and tells us if someone is sniffing through our system. Intrusion Detection System is a tool that is used by people working in big companies to people who have personal computers. IDS can be defined as a tool or application software or a device that detects and reports malicious activities in a system [3]. IDS works with the help of a SIEM (security information and event management). The intrusion in our systems and violation of the rules specified in our systems is typically collected and sent to the administrator or collected centrally using SIEM. The purpose of IDS is to collect information and send it to an authority that will fire a signal [4].

That signal will then indicate to the user that there is an intrusion in the system. Intrusion detection system identifies the intrusion and malicious activities by analyzing traffic patterns of the system. The overall function of an intrusion detection system is to analyze the traffic patterns, look for anything that is suspicious, collect the data regarding any malicious activities and then fire an alarm for the user to know that there is an intrusion in the system. Intrusion Detection System is of types such as NIDS, IDS, PIDS, APIDS, and Hybrid. NIDS (Network intrusion detection system): This IDS is placed at strategic points in a network. NIDS analyzes the traffic of all the systems present in one subnet. Depending on the rules that are configured by the network administrator or user, NIDS

ISSN: 2057-5688

analyzes the traffic pattern. NIDS also analyzes traffic patterns based on the signatures that are present in a database. Placing IDS before a firewall is an example of Network IDS [5].

2. LITERATURE SURVEY

H. R. Ghaeini, and N. O. Tippenhauer .et.al [6], in this paper, we propose a hierarchical monitoring intrusion detection system (HAMIDS) for industrial control systems (ICS). The HAMIDS framework detects the anomalies in both level 0 and level 1 of an industrial control plant. In addition, the framework aggregates the cyber-physical process data in one point for further analysis as part of the intrusion detection process. The novelty of this framework is its ability to detect anomalies that have a distributed impact on the cyber-physical process. The performance of the proposed framework evaluated as part of SWaT security showdown (S3) in which six international teams were invited to test the framework in a real industrial control system. The proposed framework outperformed other proposed academic IDS in term of detection of ICS threats during the S3 event, which was held from July 25-29, 2016 at Singapore University of Technology and Design.

Y. Xie, Y. Wang, H. He, Y. Xiang, S. Yu, and X. Liu .et.al [7], Collaborative Anomaly Detection (CAD) is an emerging fieldof network security in both academia and industry. It has attracted a lot of attention, due to the limitations of traditional fortress- style defense modes. Even though a number of pioneer studies have been conducted in this area, few of them concern about the universality issue. This work focuses on two aspects of it. First, a unified collaborative detection framework is developed based on network virtualization technology. Its purpose is to provide a generic approach that can be applied to designing specific schemes for various application scenarios and objectives. Second, a general behavior perception model is proposed for theunified framework based on hidden Markov random field. Spatial Markovianity is introduced to model the spatial context of distributed network behavior and stochastic interaction among interconnected nodes. Algorithms are derived for parameter estimation, forward prediction, backward smooth, and the normality evaluation of both global network situation and local behavior. Numerical experiments using extensive simulations and several real datasets are presented to validate the proposed solution. Performance-related issues and comparison with related works are discussed.

T. Akidau, R. Bradshaw, C. Chambers, S. Chernyak, R. Fernandez Moctezuma, R. Lax, S. McVeety, D. Mills, F. Perry,

E. Schmidt, and S. Whittle .et.al [8] Unbounded, unordered, global-scale datasets are increasingly common in day-to-day business (e.g. Web logs, mobile usage statistics, and sensor networks). At the

ISSN: 2057-5688

same time, consumers of these datasets have evolved sophisticated requirements, such as event-time ordering and windowing by features of the data themselves, in addition to an insatiable hunger for faster answers. Meanwhile, practicality dictates that one can never fully optimize along all dimensions of correctness, latency, and cost for these types of input. As a result, data processing practitioners are left with the quandary of how to reconcile the tensions between these seemingly competing propositions, often resulting in disparate implementations and systems. We propose that a fundamental shift of approach is necessary to deal with these evolved requirements in modern data processing. We as a field must stop trying to groom unbounded datasets into finite pools of information that eventually become complete, and instead live and breathe under the assumption that we will never know if or when we have seen all of our data, only that new data will arrive, old data may be retracted, and the only way to make this problem tractable is via principled abstractions that allow the practitioner the choice of appropriate tradeoffs along the axes of interest: correctness, latency, and cost. In this paper, we present one such approach, the Dataflow Model1 , along with a detailed examination of the semantics it enables, an overview of the core principles that guided its design, and a validation of the model itself via the real-world experiences that led to its development.

Wang, Ke.et.al [9], we present a payload-based anomaly detector; we call PAYL, for intrusion detection. PAYL models the normal application payload of network traffic in a fully automatic, unsupervised and very efficient fashion. We first compute during a training phase a profile byte frequency distribution and their standard deviation of the application payload flowing to a single host and port. We then use Mahalanobis distance during the detection phase to calculate the similarity of new data against the pre-computed profile. The detector compares this measure against a threshold and generates an alert when the distance of the new input exceeds this threshold. We demonstrate the surprising effectiveness of the method on the 1999 DARPA IDS dataset and a live dataset we collected on the Columbia CS department network. In once case nearly 100% accuracy is achieved with 0.1% false positive rate for port 80 traffic.

A. Sendi, M. Dagenais, M. Jabbarifar, and M. Couture.et.al [10], Cyber attacks and malicious activities are rapidly becoming a major threat to proper secure organization. Many security tools may be installed in distributed systems and monitor all events in a network. Security managers often have to process huge numbers of alerts per day, produced by such tools. Intrusion prediction is an important technique to help response systems reacting properly before the network is compromised. In this paper, we propose a framework to predict multi-step attacks before they pose a serious security

ISSN: 2057-5688

risk. Hidden Markov Model (HMM) is usedto extract the interactions between attackers and networks. Since alerts correlation plays a critical role in prediction, a modulated alert severity through correlation concept is used instead of just individual alerts and their severity. Modulated severity generates prediction alarms for the most interesting steps of multi-step attacks and improves the accuracy. Our experiments on the Lincoln Laboratory 2000 data set show that our algorithm perfectly predicts multistep attacks before they can compromise the network.

3. MULTILEVEL AUTHENTICATION SYSTEM USING HIERARCHICAL INTRUSION DETECTION ARCHITECTURE

The below figure (1) shows the flow chart of multilevel authentication system using hierarchical intrusion detection architecture. In this initially user will check client computer attacks by using phishing and Trojans techniques. By using banking services the network traffic is applied. If there are any attacks obtained then pharming, DNS spoofing and network interception techniques are applied. With the help of SSL communication network traffic is provided. Intrusion detection system will detect attacks. From banking website data will be transferred. At last online banking systems provides data and reduce errors.

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or forthcoming threats of violation of computer security policies, acceptable use policies, or standard security practices. Incidents have many causes, such as malware (e.g., worms, spyware), attackers gaining unauthorized access to systems from the Internet during Internet Banking, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized. Intrusion Detection System (IDS) is a hardware or software or combinational system, with defensive aggressive approach to protect information, systems and networks. It is usable on host, network and application levels.

It analyzes the system or network traffic or controls the incoming connections to different ports, and then it detects the occurring attacks. It can detect known attacks, unusual traffic, harmful data, misuse and unauthorized access to the systems and networksby internal users or external intruders. It informs and notifies to the security manager by different types of warnings or notifications; sometimes, it disconnects the suspicious connections or blocks malicious traffic. In general, three main functionalities of IDSs include monitoring (evaluation), analyzing (detection) and responding

ISSN: 2057-5688

(reporting) to the occurring attacks on computer systems and networks. IDSs use many methodologies to detect attacks.

Network Intrusion Detection Systems (NIDS) Network Intrusion Detection Systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, works in a promiscuous mode, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.

Host Intrusion Detection System (HIDS) Host-based IDS systems consist of software agents installed on individual computers within the system. HIDS analyze the traffic to and from the specific computer on which the intrusion detection software is installed on. HIDS systems often provide features one can't get with network-based IDS. For example, HIDS are able to monitor activities that only an administrator should be able to implement. It is also able to monitor changes to key system files and any attempt to overwrite these files. Attempts to install Trojans or backdoors can also be monitored by a HIDS and stopped. These specific intrusion events are not always seen by a NIDS.

ISSN: 2057-5688

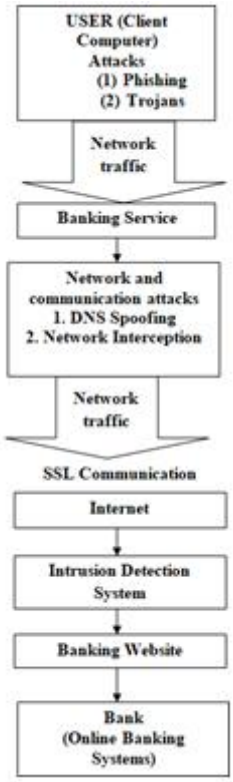

Fig. 1: FLOW CHART OF MULTILEVEL AUTHENTICATION SYSTEM USING HIERARCHICAL INTRUSIONDETECTION ARCHITECTURE

An attack can be defined as an intended or planned visit to the system by an uninvited visitor who sneaks and spoils or defaces the system or web site. Several types of electronic fraud specifically target internet banking. Some of the more popular types are described below: A. Phishing attacks Phishing attacks use fake email messages from an agency or individual pretending to represent one's bank or financial institution. The email asks to provide sensitive information (name, password, account number, and so forth) and provides links to a counterfeit web site. If one follow the link and provide the requested information, intruders can access personal account information and finances. In some cases, pop-up windows can appear in front of a copy of a genuine bank web site. The real web site address is displayed; however, any information one type directly into the pop-up will go to unauthorized users.

B. Man-in-the-middle attack (MitM) it allows the hacker to see or even to modify the communication between the client and the bank. The attacker needs to have a trojan horse virus on the victim computer

ISSN: 2057-5688

C. Man-in-the –browser attack (MitB) A MitB attack is carried out by infecting a user browser with a browser addon, or plug-in that performs malicious actions. In principle, as soon as a user's machine is infected with malware, the attacker can do anything the user can, and can act on their behalf. If a user logs into their bank account while infected, the attacker can make any bank transfer that the user can. By the virtue of being invoked by the browser during Web surfing, that code can take over the session and perform malicious actions without the user's knowledge.

D. Spyware Spyware is another way through which online banking credentials are stolen and used for fraudulent activities. Spyware works by capturing information either on the computer, or while it is transmitted between user's computer and websites. Often times, it is installed through fake "pop up" ads asking users to download software.

E. Viruses Viruses are designed to compromise your computer systems, and allow others to gain access to your files, etc. This is different than spyware in that a virus may search for information considered to be of value, where spyware will wait for input or action from whomever is using the computer. A system that is compromised may be used to attack other systems, denying people legitimate access to services. These types of attacks are called "denial of service" attacks. One of the most common scenarios with viruses is where they will discover financial data such as payroll files, bank account information, and credit card information.

F. Keylogger Trojan attacks These „keyboard spying" programs will monitor activity on the victim"s computer and wait for the user to connect to an actual banking website. As soon as the user accesses a banking website – that is on the Trojan"s list of bank sites – the Trojan virus will start to capture the keystrokes that the user types on their keyboard. This enables the cybercriminal to steal data – including login, username, and password – which then enables the criminal to access the user"s account and transfer funds.

4. RESULTS AND DISCUSSION

The below table (1) shows the comparison of Single Level Authentication System Using Hierarchical Intrusion Detection Architecture and Multilevel Authentication System Using Hierarchical Intrusion Detection Architecture. In this accuracy, precision, f1-score, security, attacks and time duration parameters are utilized. Compared with Single Level Authentication System Using Hierarchical Intrusion Detection Architecture, Multilevel Authentication System Using Hierarchical Intrusion Detection Architecture improve accuracy, precision, F1-Score, security and reduce the attacks and time duration to perform the entire operation.

ISSN: 2057-5688

Table. 1: COMAPRISON TABLE

S.NO	Parameter	Single Level Authentication System Using Hierarchical Intrusion Detection Architecture	Multilevel Authentication System Using Hierarchical Intrusion Detection Architecture
1	Accuracy	73%	91%
2	Precision	78%	89%
3	F1-Score	63%	82%
4	security	81%	97%
5	Attacks	86%	12%
6	Time duration	72%	9%

The below figure (2) shows the comparison of accuracy for both Single Level Authentication System Using Hierarchical Intrusion Detection Architecture and Multilevel Authentication System Using Hierarchical Intrusion Detection

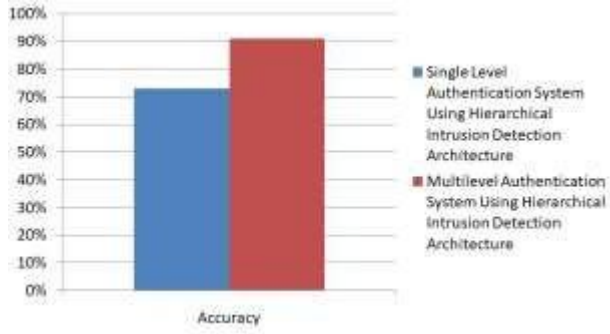

Fig. 2: COMPARISON OF ACCURACY

The below figure (3) shows the comparison of precision for both Single Level Authentication System Using Hierarchical Intrusion Detection Architecture and Multilevel Authentication System Using Hierarchical Intrusion Detection

ISSN: 2057-5688

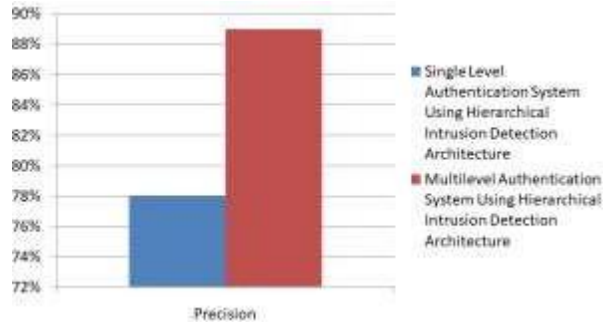

Fig. 3: COMPARISON OF F1-SCORE, SECURITY, TIME DURATION

The below figure (4) shows the comparison of F1 score for both Single Level Authentication System Using HierarchicalIntrusion Detection Architecture and Multilevel Authentication System Using Hierarchical Intrusion Detection.

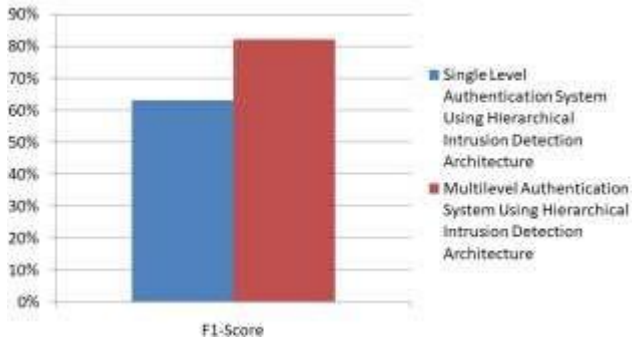

Fig. 4: COMPARISON OF F1-SCORE

The below figure (5) shows the comparison of security for both Single Level Authentication System Using Hierarchical IntrusionDetection Architecture and Multilevel Authentication System Using Hierarchical Intrusion Detection.

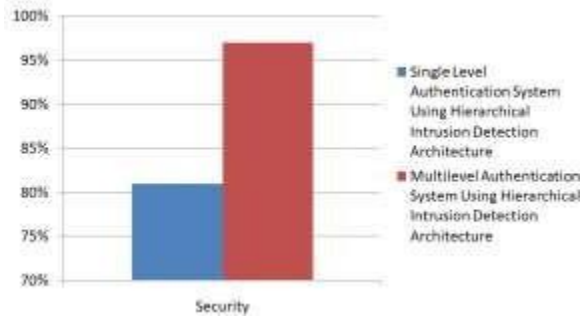

Fig. 5: COMPARISON OF SECURITY

The below figure (6) shows the comparison of attacks for both Single Level Authentication System

ISSN: 2057-5688

Using Hierarchical Intrusion Detection Architecture and Multilevel Authentication System Using Hierarchical Intrusion Detection.

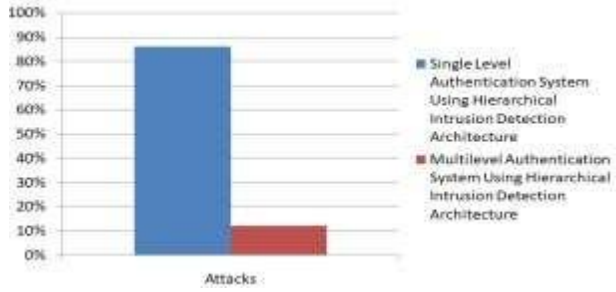

Fig. 6: COMPARISON OF ATTACKS

The below figure (7) shows the comparison of time duration for both Single Level Authentication System Using Hierarchical Intrusion Detection Architecture and Multilevel Authentication System Using Hierarchical Intrusion Detection.

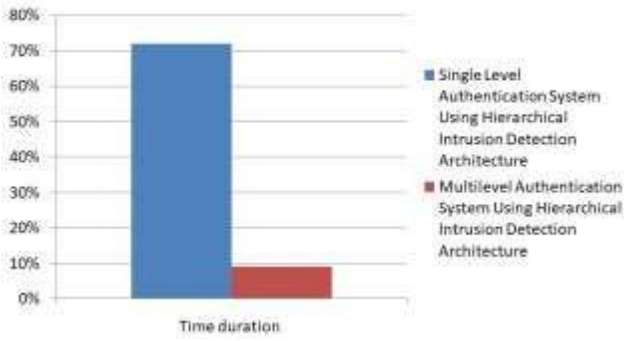

Fig. 7: COMPARISON OF TIME DURATION

5. CONCLUSION

Nowadays internet has a key role in interaction between peoples and their businesses (such as banking). One of domain which uses this new communication channel for more and better interacts with its customers is online-banking (OB) industry. Using of OB is increasing rapidly. the significant growth in presenting and using of OB services such as responding to customers' requests on every time and every place and additive integration, leads to fast growth in fraud events and security problems. One of solutions against to security problems into this domain is using secure protocols. Also, it is possible to add new security layers like intrusion detection to the OB security infrastructure. With the growth in popularity of online banking services, the theft of banking information has become one of the most common types of criminal activity on the Internet. Internet banking continues to present challenges to financial security and personal privacy. This paper suggests using Intrusion

Detection System in Internet Banking security infrastructure for increasing the security of Online banking transactions. The most important advantages ofusing IDS as security solution for banks is that they increase safety and reliability of Internet Banking services and decrease the damages of fraud events. From results

6. REFERENCES

[1] C. Fu, Q. Li, M. Shen, and K. Xu, ”Realtime robust malicious traffic detection via frequency domain analysis,” in Proc. 2021 ACM SIGSAC Conf. on Comm. and Comp. Security, Nov. 2021.

[2] O. Alkadi, N. Moustafa, B. Turnbull, and K. Choo, ”A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks,” IEEE Internet of Things Journal, May 2020.

[3] R. Sibai, Y. Chabchoub, C. Jaoude, J. Demejian, and M. Togbe, ”Towards efficient data sampling for temporal anomaly detection in sensor networks,” in Proc. IEEE MENACOMM 2019, Nov. 2019.

[4] P. Halgodo, V. Villagra, and L. Vazquez, ”Real-time multistep attak predeiction based on hidden Markov models,” IEEE Trans. Dep. Sec. Comp., vol. 17, no. 1, pp. 134-147, 2017.

[5] W. Meng, ”Intrusion detection in the era of IoT: building trust via traffic filtering and sampling,” IEEE Computer, vol. 51, no. 7, pp. 36-43, 2018.

[6] H. R. Ghaeini, and N. O. Tippenhauer,”HAMIDS: Hierarchical monitoring intrusion detection system for industrial control systems,” in CPS-SPC 2016, Oct. 2016.

[7] Y. Xie, Y. Wang, H. He, Y. Xiang, S. Yu, and X. Liu, ”A general framework for modeling and perceiving distributed network behavior,” IEEE/ACM Trans. on Netw., vol. 24, no. 5, pp. 3162-3176, Oct. 2016.

[8] T. Akidau, R. Bradshaw, C. Chambers, S. Chernyak, R. Fernandez Moctezuma, R. Lax, S. McVeety, D. Mills, F. Perry, E. Schmidt, and S. Whittle, “The dataflow model: a practical approach to balancing correctness, latency, and cost in massive-scale, unbounded, out-oforder data processing,” in Proc. VLDB Endowment, vol. 8, no. 12, 2015

[9] Wang, Ke. "Anomalous Payload-Based Network Intrusion Detection". Recent Advances in Intrusion Detection. Springer Berlin, 2013 doi:10.1007/978-3-540-30143-1_11

[10] A. Sendi, M. Dagenais, M. Jabbarifar, and M. Couture ”Real time intrusion prediction based on optimized alerts with hidden Markov model,” J. Netw., vol. 7, no. 2, pp. 311-321, 2012.

ISSN: 2057-5688

[11] H. Farhadi, M. AmirHaeri, and, M. Khansari, ”Alert correlation and prediction using data mining and HMM,” ISC Intl. J. Info. Secur., vol. 2, no. 2, pp. 77-101, 2011.

[12] K. Haslum, M. Moe, and S. Knapskog, ”Real-time intrusion prevention and security analysis of networks using HMMs,” in Proc. 2008 Intl. Conf. Local Comp. Netw., 2008.

[13] Uyyala P. COLLUSION DEFENDER PRESERVING SUBSCRIBERS PRIVACY IN PUBLISH AND SUBSCRIBE SYSTEMS. The International journal of analytical and experimental modal analysis. 2021;13(4):2639-45.

[14] Uyyala, Prabhakara. "Delegated Authorization Framework for EHR Services using Attribute Based Encryption." *TheInternational journal of analytical and experimental modal analysis* 13, no. 3 (2021): 2447-2451.