Two Step Authentication for an Anomaly based Intrusion Detection System

Nikhil Vijaywar
M.Tech. Scholar,
Oriental College of Technology
Bhopal, India.

Vivek Kumar
Assistant Professor,
Oriental College of Technology
Bhopal, India.

ABSTRACT

Intrusion detection is an effective approach of dealing with problems in the area of network security. Rapid development in technology has raised the need for an effective intrusion detection system as the traditional intrusion detection method cannot compete against newly advanced intrusions. As most IDS try to perform their task in real time but their performance hinders as they undergo different level of analysis or their reaction to limit the damage of some intrusions by terminating the network connection, a real time is not always achieved. The system implements the detection algorithm as a Snort preprocessor component. Since they work together, a highly effective system against unknown threats (which was the main aim of the designed system.).

Keywords

Anomaly, Bloom Filter, IDS, Intrusion Detection System, Malware, N-Gram, NIDS, Payload, Preprocessor, Network Intrusion Detection System, Snort.

1. INTRODUCTION

Intrusion detection is a network security mechanism to protect the computer network system from invasion or attacks. Advancement in network technologies has provided an opening to hackers and intruders to find unauthorized ways to enter into a new system. Therefore, as technologies evolve, there is also a risk of new threats existing with them. Thus, when a new type of invasion emerges, an intrusion detection system (IDS) needs to be able to act effectively and in a timely manner in order to avoid hazardous effects. In today’s context, the biggest challenge could be dealing with ‘big data’, i.e., a huge volume of network traffic data that gets collected dynamically in the network communications [1]. Therefore, intrusion detection has been one of the core areas of computer security whose objective is to identify these malicious activities in network traffic and, importantly to protect the resources from the threat. Most IDS try to perform their task in real time but they lack due to various reasons. The circumstances like degree of analysis and computation it needs to undergo, the real time performance is not always possible.The primary function of the IDS is to protect the Confidentiality, Integrity, and Availability (CIA) of information and information systems. It is an integral part of well managed comprehensive security enclave. The IDS is a vital tool as the degradation or non availability of network resources could be detrimental to business, particularly as network applications and protocols become vulnerable to attacks. While the IDS cannot provide total security, it is a means to deter malicious attacks from propagating freely throughout networks. In general, IDSs are separated into two broad categories. Anomaly-based systems compare attack-free data to network traffic where anomalous events are identified as deviations from the norm, while misuse-based systems match signatures or unique character strings to known attacks. This study focuses on anomaly detection, where specially designed systems analyze packet data content for anomalous or suspicious activity. The purpose of this thesis is to determine whether payload anomaly-based IDSs are effective at detecting malicious attacks.

Anomaly detection is a challenging problem that has been researched within a variety of application domains such as image processing, fault isolation, fraud detection, and network intrusion detection. In network intrusion detection, anomaly based techniques are particularly attractive because of their ability to identify previously unknown attacks without the need to be programmed with the specific signatures of every possible attack. There is a significant body of work in anomaly based intrusion detection applying statistical analysis, data-mining, and machine learning disciplines.

Revolutions in communications and information technology have given birth to a virtual world. With the growth of cyberspace and its potential, there has been a subsequent change in every facet of daily life. In today’s information age, everything we do relies on access to information networks. The internet is used in the home to shop, pay bills, and stay connected via social networks. National infrastructure relies on information networks to deliver oil and gas, power and water. They support hospitals and schools, public transportation and air traffic control. Businesses are relying more and more on e-commerce. As the use of cyberspace grows, the need to protect it also grows.

2. DETECTION TECHNIQUES

The Various techniques are in place for intrusion detection which can be broadly classified as follows.

2.1 Signature/Pattern Based Detection

In this technique, the sensors which are placed in different LAN segments filter and analyze network packets in real time and compare them against a database of known attack signatures. Attack signatures are known methods that intruders have employed in the past to penetrate a network. If the packet contents match an attack signature, the IDS can take appropriate countermeasure steps as enabled by the network security administrator. These countermeasures can take the form of a wide range of responses. They can include notifications through simple network management protocol (SNMP) traps or issuance of alerts to an administrator’s email or phone, shutting down the connection or shutting down the system under threat etc.

2.2. Unauthorized Access Detection

In unauthorized access detection, the IDS detect attempts of any access violations. It maintains an access control list (ACL) where access control policies for different users based on IP addresses are stored. User requests are verified against the ACL to check any violations.

2.3.Behavioral Anomaly (Heuristic based) Detection

In behavioral anomaly detection method, the IDS are trained to learn the normal behavioral pattern of traffic flow in the network over an appropriate period of time. Then it sets a baseline or normal state of the network's traffic, protocols used and typical packet sizes and other relevant parameters of network traffic. The anomaly detector monitors different network segments to compare their state to the normal baselines and look for significant deviations.

2.4.Protocol Anomaly Detection

With this technique, anomaly detector alerts administrator of traffic that does not conform to known protocol standards. As the protocol anomaly detection analyzes network traffic for deviation from standards rather than searching for known exploits there is a potential for protocol anomaly to serve as an early detector for undocumented exploits.

3. METHOD

In the proposed scheme, an image owner having a low computational power (e.g., mobile devices) connects to the cloud. The user desires to use the storage capacity and cloud computational power. She/he stores the images securely and wants to retrieve or access them afterwards. The image owner has a collection of his sensitive images. However, the image owner wants that his collection must be secure enough before outsourcing to the cloud for further processing. Figure 1 shows the System framework of proposed algorithm. In this figure only encryption algorithm has been explored. User authentication using image captcha is explored in section while reusing the system framework of Figure 1.

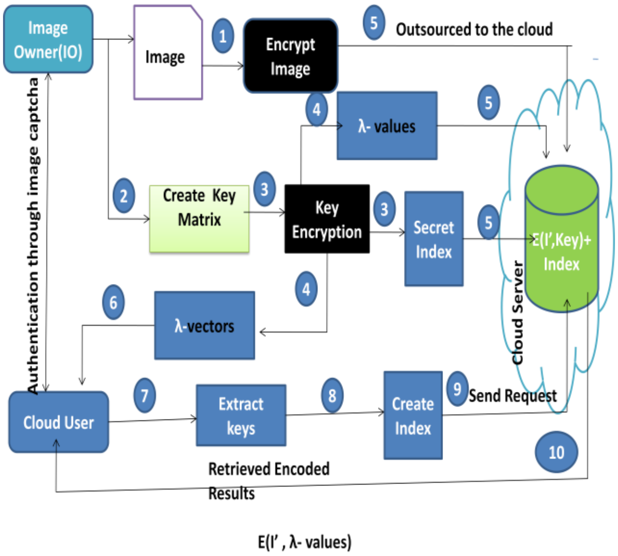


Fig.1 System framework

Proposed encryption algorithm consists of the two main tasks. The first is the Image Encryption and the second is the Key Encryption.

3.1 Image Encryption

A new image encryption algorithm with key encryption is suggested in the proposed work, different from others have proposed so far. The original color image is first mixed with the image obtained from the social media (Flicker) by using the flicker ID (flk_ID). Two hash functions h1 (z) and h2(x, y, z) have been used here, to create the flk_ID. These hash functions depend upon the features of the original image. Image encryption algorithm is shown in below, in which step by step procedure is explained. Figure 2 shows the basic structure of encryption process.

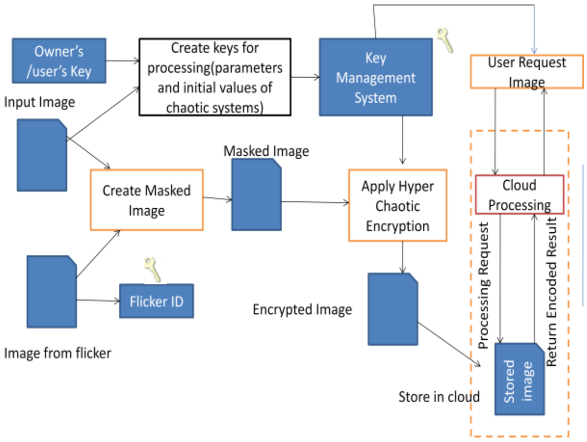


Fig.2 Basic structure of encryption process

3.2 Image Decryption

Decryption will be done by using the keys as in matrix A. Decryption process is to perform all the operations in reverse. In figure 3 flow diagram of Decryption Algorithm shown in which all steps taken for decrypt image is given with encryption also. First step is take input image and then Encrypted image is taken place which is Xoring with the Hyper chaotic user key and then it gate reshaped the whole image and then anti shuffle column and row pixel is take placed consecutively and then anti permute blocks are placed before the removal mask flicker by the use of Flicker ID then original image is taken as a output.

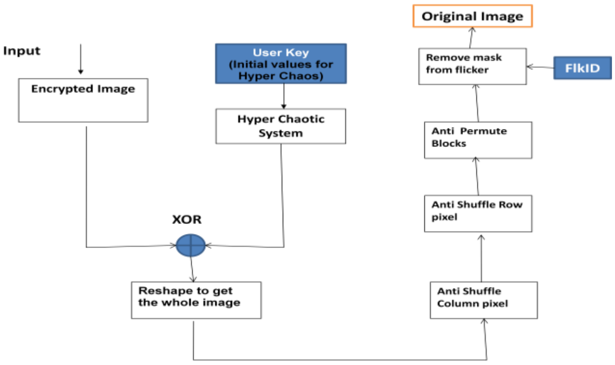


Fig. 3: Flow diagram of Decryption Algorithm

4. RESULT

Result shows the representation of all stage of the proposed work with graphical representation.

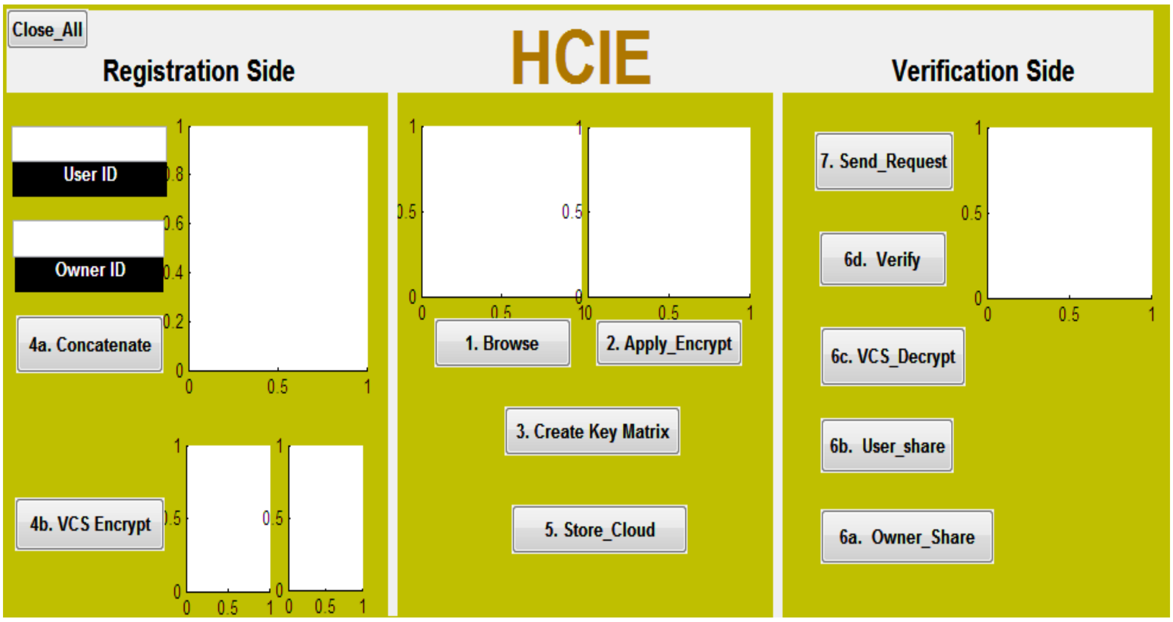
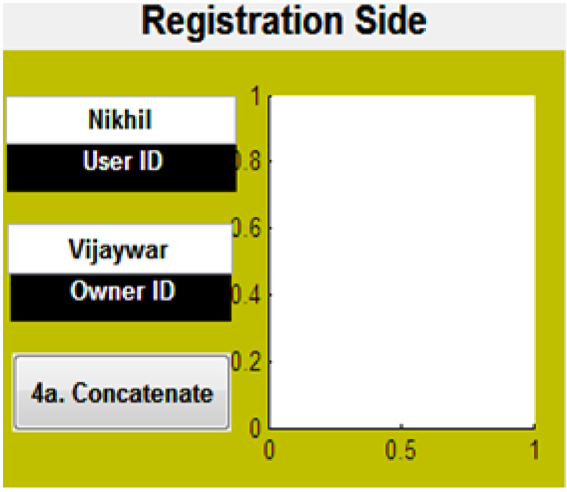


Fig.4 HCIF window

Figure 4 the window of HCIF which is used in MATLAB for the implementation of the proposed work.



Nikhil
User ID

Vijaywar
Owner ID

Fig.5 Registration side for input Id

Figure 5 shows the use of first step which is known as the registration side of the user in which user enters his/her ID then concatenate its identification after that encryption is take place; VCS encryption is take place in proposed work.

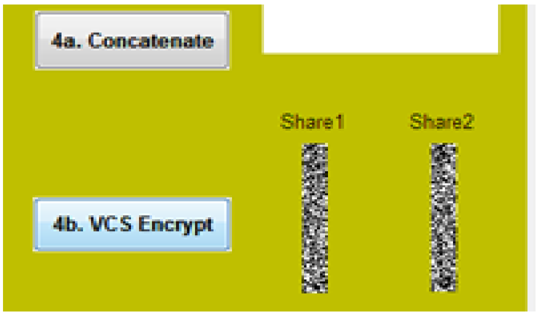


Fig.6 After VCS encrypt show the shares

Figure 6 Shows After encryption output is divided into two shares which is also shown on window in registration side.

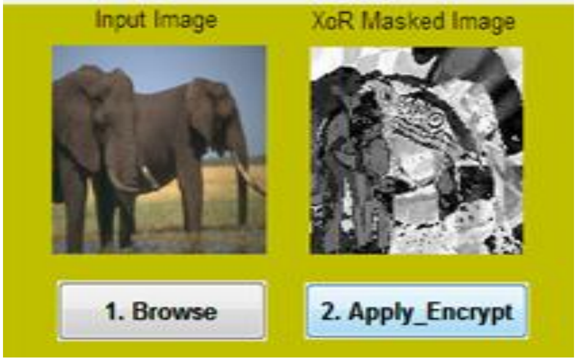
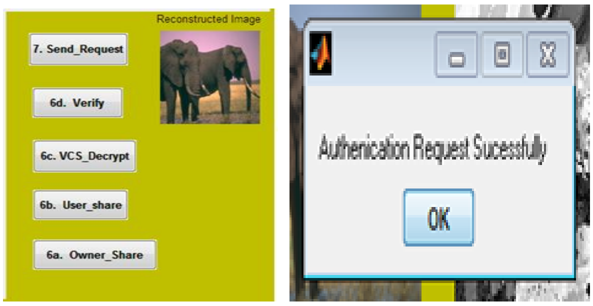


Fig. 7 Apply encrypt on input image

After sharing process user take input image for transmission by browsing procedure and then encrypted image is applied on input image which gives key matrix and also store data in cloud server and all process is taken like owner shares user shares and VCS decryption technique step by step and verification is done before sending request.



Authenication Request Sucessfully

Fig.8 authentication request

After all process verification side verify input image then a message is come as pop up window authentication request successfully and then input image is reconstructed.

5. CONCLUSION AND FUTURE SCOPE

In this paper, we present our proposal to advance the state of the art in intrusion detection. Network Intrusion Detection System has a major role to play in safeguarding the network resources against various kinds of attacks. With the advent of new vulnerabilities and sophistications in the nature of attacks, new techniques for intrusion detection have evolved. The main objectives of the research being increasing the detection accuracy while keeping the false positive rate low. A future research direction would be to find ways for a data owner to hold accountable any member that carries out malicious activities on their data. Another research direction would be to give the data owner physical access control over the data.

6. REFERENCES

[1] L. J. G. Villalba, A. L. S. Orozco and J. M. Vidal. “Anomaly-Based Network Intrusion Detection System”, IEEE Latin America Transactions, Vol. 13, No. 3, March 2015

[2] Okane, Philip, et al. "Malware detection: program run length against detection rate." IET software 8.1 (2014): 42-51.

[3] Wu, B., Lu, T., Zheng, K., Zhang, D., & Lin, X. Smartphone “malware detection model based on artificial immune system”. China Communications, 11(13), 86-92.

[4] Uppal, D., Sinha, R., Mehra, V., & Jain, V. (2014, September). “Malware detection and classification based on extraction of API sequences” In Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on (pp. 2337-2342). IEEE.

[5] He, Daojing, Sammy Chan, and Mohsen Guizani. “Mobile application security: malware threats and defences” IEEE Wireless Communications 22.1 (2015): 138-144.

[6] D. Bolzoni, S. Etalle, P. Hartel, E. Zambon. POSEIDON : a 2- tier “Anomaly based network intrusion detection system”, IEEE april 2006.

[7] Artificial immune system based general purpose intrusion detection system. Technical report, January 2009.

[8] S. B. Medhdi, A. K. Tanwani, M. Farooq. IMAD: In execution malware analysis and detection. GECCO july 2009.

[9] J. Jung, V. Paxson, A. W. Berger, H. Balakrishnan “Fast portscan detection using sequential hypothesis testing”, IEEE may 2004.

[10] Y. Gu, A. McCallum, D. F. Towsley “Detecting anomalies in network traffic using maximum entropy estimation”, oct.2005.

[11] Garcia-Teodoro, Pedro, et al. "Anomaly-based network intrusion detection: Techniques, systems and challenges." computers & security 28.1 (2009): 18-28.