Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7778276

AUTHENTICATION BASED SUSPICIOUS BEHAVIOUR DETECTION SYSTEM ONTHE CLOUD.

Sandeep Kaur
Ph.D Scholar, Sri Guru Granth Sahib World University, FGS.
Sandeep18033@gmail.com

Sarpreet Singh
Assistant Professor, Sri Guru Granth sahib World University, FGS.
ersarpreetvirk@gmail.com

ABSTRACT

Secure authentication is essential in the cloud since anyone might attempt to enter into your account from anywhere on the internet. However, even after you've taken every precaution to secure it, someone may still gain access to your cloud administration layer, including the APIs that lead to the leakage of keys or accounts. Therefore, intrusion detection at the cloud layer, which is above the computing layer, is crucial. By implementing an authentication-based intrusion detection system, cloud computing platforms cannot only ensure that legidmate users are accessing resources and data on the cloud, also detect malicious activity that can cause leading cyber attacks, and other security incidents that can result in financial loss, reputational damage, and legal liabilities. To circumvent the above menthioned threats, this study proposed an Authentication Based Suspicious Behavior Detection System that to do intrusion detection at the cloud layer that explores the API. A knowledge-based (Kbase) dataset is used to detect the authentication phase allied attacks. Simulation practices of multiple cracking tasks demonstrate the applicability of the approach.

INTRODUCTION

Authentication is crucial to the general safety of software programmers and computer systems. Its main function is to prevent unauthorized users from accessing the system and to make sure that authorized users have access to the resources they require. It is commonly believed that passwords are the key to authentication. But safeguarding a software program or system heavily relies on the authentication procedure. The use of user authentication systems is widespread in daily life. Unfortunately, existing authentication systems are vulnerable to various attacks, and both system security and usability are expected to be satisfied. [1]. Hence securing authentication process itself, becomes an even important and imperative task [2][3]. It's also critical to realize that authentication by itself cannot fully secure a system. It has to be connected to IDS. There are many benefits to building IDS on top of the cloud environment. A hardware or software intrusion detection system typically examines incoming and outgoing network data for indications of malicious activity. IDS focus on a former analysis of all user requests and system actions. The system requires the recording of all user requests and activities for their later analysis. IDS controls are useful both as deterrent against misbehavior as well as a means to analyze the user's behavior in using the system to find out about possible

attempted or actual violations. Authentication and intrusion detection together provide the foundations for building systems which can store and process information with confidentiality and integrity[4].

Nowadays most of the CSPs are using IDS to secure cloud data. An intrusion detection model Security as a service (SAAS) in Cloud had already been investigated by many researchers. But there is no such standard framework or architecture developed for setting up IDS with authentication framework[3]. Authentication is the primary security service. Both IDS and strong authentication supports good auditing because operations can then be traced to the user who caused them to occur. There is a mutual interdependence between these technologies which can be often ignored by security practitioners and researchers[4].

Moreover, there are many benefits to building IDS on top of the cloud environment. Cloud environments make it possible to identify harmful network activity from a variety of angles and fix the traditional intrusion detection problem [5]. In the cloud computing environment, need to switch in different layers to do intrusion detection [20]. Both the network layer and virtual machines depend on the cloud layer. The network and computing layers may be affected by whoever manages access to the cloud management layer. We need intrusion detection at three different layers[20]:-

Cloud layer: This layer is responsible for providing the overall cloud infrastructure, including the physical servers, storage, and network resources. It includes the data centers and hardware components required to host cloud services.

Network layer: This layer is responsible for managing the networking infrastructure required to connect cloud resources together. It includes the routers, switches, load balancers, and other network components required to route traffic between different cloud services and to provide connectivity to the internet.

Compute Layer(Virtual Machines, Containers, etc.)[20]: This layer is responsible for managing the processing power required to run cloud applications and services. It includes the virtual machines, containers, and other compute resources required to execute code and run applications.

Cloud Layer explores API logs. Authentication APIs are used to authenticate and authorize users and applications to access cloud resources. They allow users to securely log in to the cloud management layer and perform various tasks, such as creating virtual machines or deploying applications. Secure authentication API in the cloud is essential as anyone can try to log into your account from anywhere However, even if you have secured it as well as possible, people can still get into your cloud management layer, including APIs, resulting in the loss of keys or accounts. Therefore, it's crucial to scan the cloud layer for the detection and prevention the intrusions [20]. This method needs to be applied more in intrusion detection systems in the future. A signature database, service console, and analysis engine make up the cloud-based IDS for speeding up analysis. The adoption of cloud-based IDSs should increase in the near future even if it is still in its infancy [5].

Moreover, there is a need to update the underlying dataset to identify the recent attacks in the field of IDS with improved detection. Eliminating all the irrelevant data from training dataset is a better way to enhance the classification accuracy and yield a proficient IDS [4]. Furthermore, self-generate dataset and private datasets can be prepared for specific experiment and better address particular needs [6]. Besides, as normal activities are frequently changing

and may not remain effective over time, there exist a need for newer and more comprehensive datasets that contain newly emerging malware activities. A new malware dataset is needed, as most of the existing machine learning techniques are trained and evaluated on the knowledge provided by the old dataset such as DARPA/ KDD99, which do not include newer malware activities. Therefore, only these datasets are publicly available and no other alternative and acceptable datasets are available. Though ADFA dataset contain many new attacks, it is not adequate[7]. For that reason, testing using these datasets does not offer a real evaluation and could result in inaccurate claims for their effectiveness. Developing IDSs capable of overcoming the evasion techniques remains a major challenge for this area of research[7]. The types of network attacks changed over the years, and therefore, there is a need to update the datasets used for evaluating IDS [15].Though, in a dynamically changing computing environment, IDS needs a regular update on knowledge for the expected abnormal behavior, has the capability to reduce false-positive alarms since the system has knowledge about all the abnormal behaviors[7]. This study focus on the need and designing of the authentication based suspicious behavior detection system and required dataset.

LITERATURE REVIEW

Authentication is not an aggregated solution for securing a system [4]. Intrusions are becoming more common and pose a serious threat to computer systems, including Cloud. An intrusion is any unauthorized access to a computer and its resources that compromises the confidentiality, integrity, or availability of the system. Intrusions can have harmful effects on the computer system. An Intrusion is carried out by launching successful attacks. Examples of attacks are Malware attack, Denial of Service (DoS) attack, Distributed DoS (DDoS) attack, Phishing attack, SQL Injection attack, Brute force attack, Data leakage attack, Spoofing attack. Research scholars have done analysis on security attacks in cloud platform in order to capture complex attacks [7]. In the study [8], secure authentication framework circumvent the security issues on the vulnerable channel. It is also important to understand that authentication is not a complete solution for securing a system. It must be coupled with IDS. The system requires the recording of all user requests and activities for analysis. IDS controls are useful both as deterrent against misbehavior as well as a means to analyze the users behavior in using the system to find out about possible attempted or actual violations. Nowadays most of the CSPs are using IDS to secure cloud data. IDS analyses the network and checks for any malicious activity. If malicious activity occurs, it alerts the network administrator at once. To classify all the attacks from dataset a proficient IDS is required. Eliminating all the irrelevant data from training dataset is a better way to enhance the classification accuracy and yield a proficient IDS[4].The study [9] proposes NK-RNN model and packet securitization algorithm. The algorithm examines the packets from the users. For preventing the user from intruders, they proposed a one-time signature for cloud user in order to access the data on cloud environment. The classifier effectively detects the intruders which are experimentally proved by comparing with existing classification. They point out the complications of vulnerable intruders and also furnished efficacious solutions in order to solve problem of intruders such as DDOS, probe, U2R, R2L and zero day [9]. Another proposed architecture eradicates malicious behaviors by detecting known attacks using log files, blocks suspicious behaviors in real time on behalf of recent architectures requests, secures sensitive data, and establishes better adaptations of security

measures by dynamically updating security rule[10].An expert system comprises a number of rules that define attacks. In an expert system, the rules are usually manually defined by a knowledge engineer working in collaboration with a domain expert [11].These are knowledge base techniques or expert system require create a knowledge base which is used to detect the intrusion. The standard file is normally created based on human knowledge, in terms of a set of rules that try to define normal system activity. The main benefit of knowledge-based techniques is the capability to reduce false-positive alarms since the system has knowledge about all the normal behaviors. Another language-based intrusion detection approach defines the syntax of rules which can be used to specify the characteristics of a defined attack. Rules could be built by description languages such as N-grammars and UML in it[12]. The knowledge base reflects the legitimate traffic profile. Actions which differ from this standard profile are treated as an intrusion. The standard profile model is normally created based on human knowledge, in terms of a set of rules that try to define normal system activity. The main benefit of knowledge-based techniques is the capability to reduce false-positive alarms since the system has knowledge about all the normal behaviors. However, in a dynamically changing computing environment, this kind of IDS needs a regular update on knowledge for the expected normal behavior which is a time consuming task as gathering information about all normal behaviors is very difficult[11]. Moreover, the approaches find the deviation between known and unknown behavior which is inadequate for detecting the other types of attacks. Although there are several approaches to intrusion detection, such as signature-based and anomaly-based, machine learning (ML) based approaches have emerged as a recent interest and research area. A robust IDS needs a reliable and up-to-date dataset in order to capture the behaviors of the new types of attacks [19]. With their robust learning models, and data centric approach, ML based security solutions for cloud environments have been proven effective [13][14].Machine learning-based security approaches are likely vulnerable to poisoned datasets which can be caused by a legitimate defender's misclassification or attackers aiming to evade detection by contaminating the training data set[5].Traditionally, in data center environments, people conduct intrusion detection at the network layer, using tools like Zeek and Snort. These tools process raw network traffic data and then pattern-match for specific signatures, behaviors or anomalies [6]. However, in the cloud, it's not as easy to get a copy of the raw network traffic due to the limitations of the environment. The cloud provider typically hosts multiple customers, and is responsible for the physical network, meaning customers do not get direct access to it. Therefore, in the cloud, we must switch to different layers to do intrusion detection [6].

PROPOSED AUTHENTICATION BASED SUSPICIOUS BEHAVIOR DETECTION SYSTEM. (ABSBDS)

The motivation behind this strategy is that suspicious activities should be failed, which may be an intrusion at the initial phase of communication. However, even if authentication system is strong enough, attackers can still get into your cloud management layer, including APIs, resulting in the loss of keys or accounts [20]. Therefore, it's essential to scan the cloud layer for intrusions. The integration of IDS at the cloud layer identifies the attacks to circumvent the threats before to move to the compute layer. The solution identifies the attack before it could manipulate its activity traces as normal during the authentication phase. The knowledge-based

dataset is prepared for specific experiment for addressing particular needs.It includes divulgeing of malicious payloads on the cloud layer.

The proposed Authentication based Suspicious Behavior Detection System (ABSBDS) model is shown in figure 1.

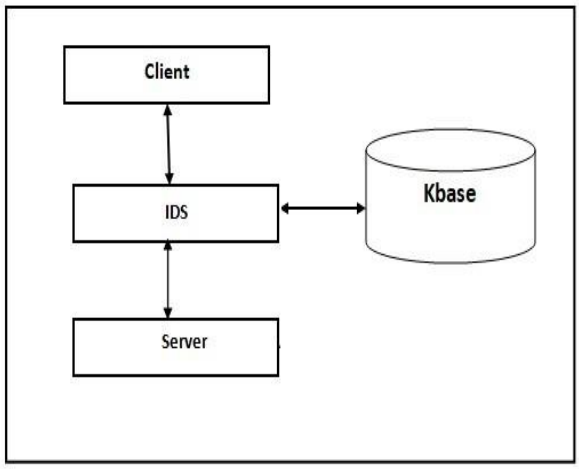

Figure 1 ABSBDS

The types of network attacks changed over the years, and therefore, there is a need to update the datasets used for evaluating IDS. In a dynamically changing computing environment, this kind of IDS needs a regular update on knowledge for the expected abnormal behavior. The distinguishing feature of the proposed work from its counterpart's is creation of an indigenous knowledge-based (Kbase) database for intrusion activities instead of standard data sets. Unlike the other classes of IDS, the K-base is created based on captured knowledge, in terms of data streams and a set of rules that define malicious system activity. The Web data stream which contains text related to the attacks/vulnerabilities, provides useful information related to the attacks. This unstructured text data is parsed into named entities which can be used to enrich the knowledge-base with structured text data like well-defined attack/attack descriptions. The integration and inference over this aggregated data can enable better detection of complex attacks[16]. The solution has the capability to reduce false-positive alarms since the system is enriched with authentication phase attack patterns. The knowledge-based data set can be easily updated as well as new attack patterns are founds. Currently knowledge base dataset is build up with SQLi attacks, Scripting attacks and other miscellaneous malicious attacks patterns that are occurring on the authentication phase.SQL injection: one of the code that may destroy your database by injecting thorough input web page. An attacker injects the malicious code, when user is asked for the user login ID and password [19]. The attack occurs, when user input is directly putting as SQL statement and it is not getting validated [17].Scripting Attacks: The attacks that are passed in script form for particular functions are known as scripting attacks. JavaScript injection on the target site - If an attacker can execute JavaScript on a page, they can do anything the user can legitimately do. An attacker finds a vulnerable web login/registration page and crafts a phishing email with XSS payload injected into the vulnerable web page and sends it to the victim [20] [23].

SIMULATION AND DISCUSSION

The simulation have been performed using a Windows 10 – 64 bits PC with 8 GB RAM and SSD 256 GB and Intel(R) Core(TM) i3-2330M CPU. For simulation, we use Hyper-V to create and run three virtual machines as shown in figure 1 and 2.

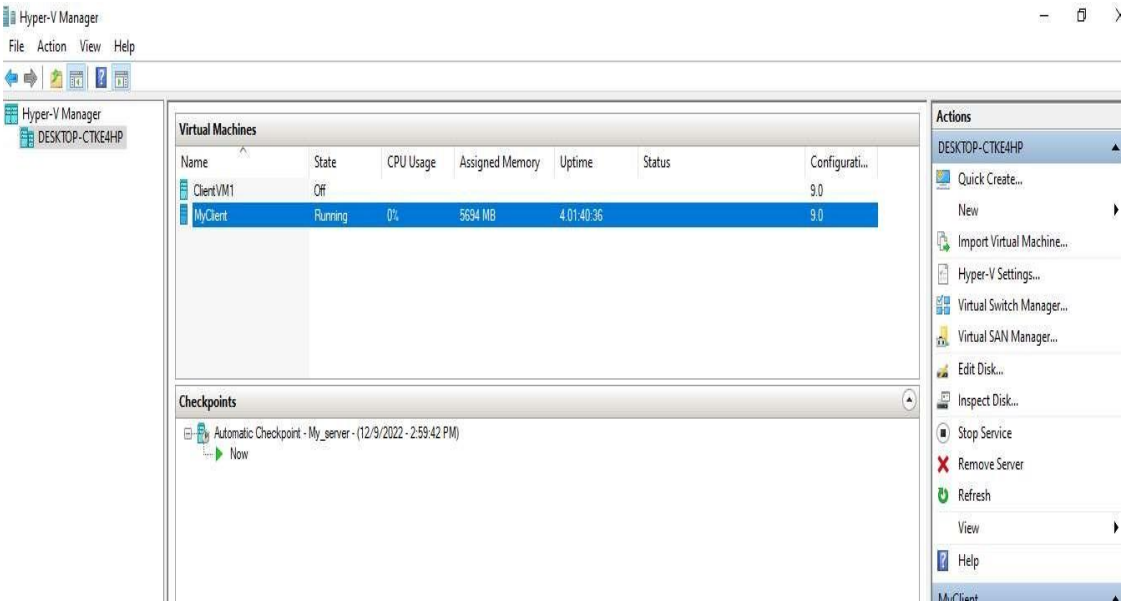

Figure 1.

Each virtual machine acts like a complete computer, running different operating system and programs as revealed in figure 2.Then we have implemented a proposed solution with Java (JDK 1.6) and NetBeans IDE 8.2. The series of experiments were achieved by applying different attack via different virtual machines. Attacks are being detected during both steps of verifications. In case of malicious code, system generates an alert. Exercises are successfully completed by exporting the SQL attack in the authentication phase.

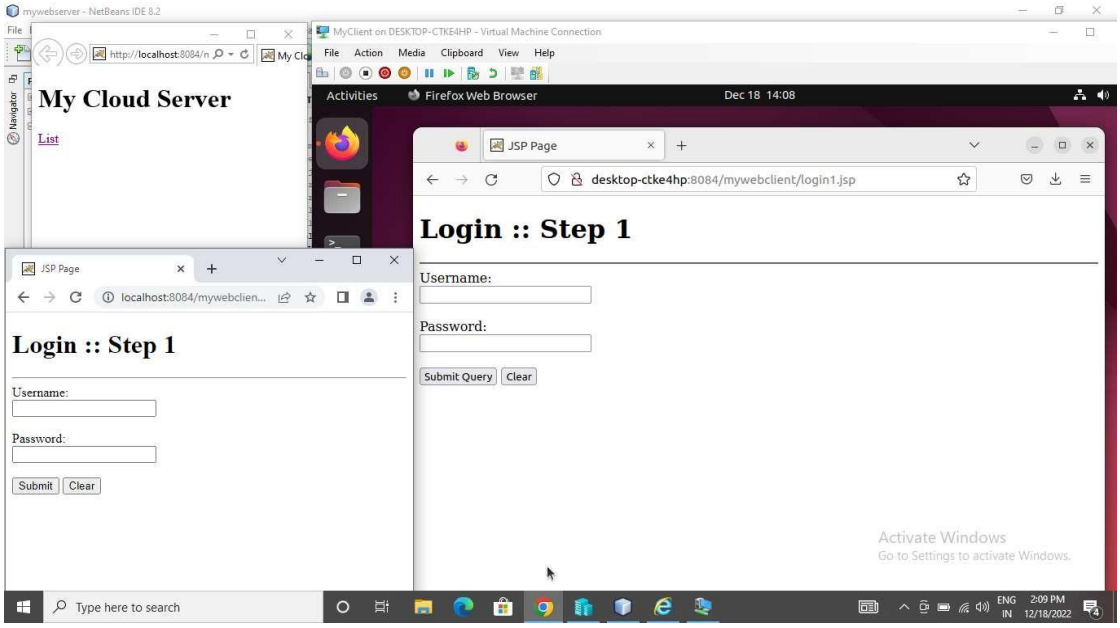

Figure 2

Figure 3 demonstarte the SQL attack structure and figure 4 show the failour attempt of the attack in the course of the first factor of authentication.

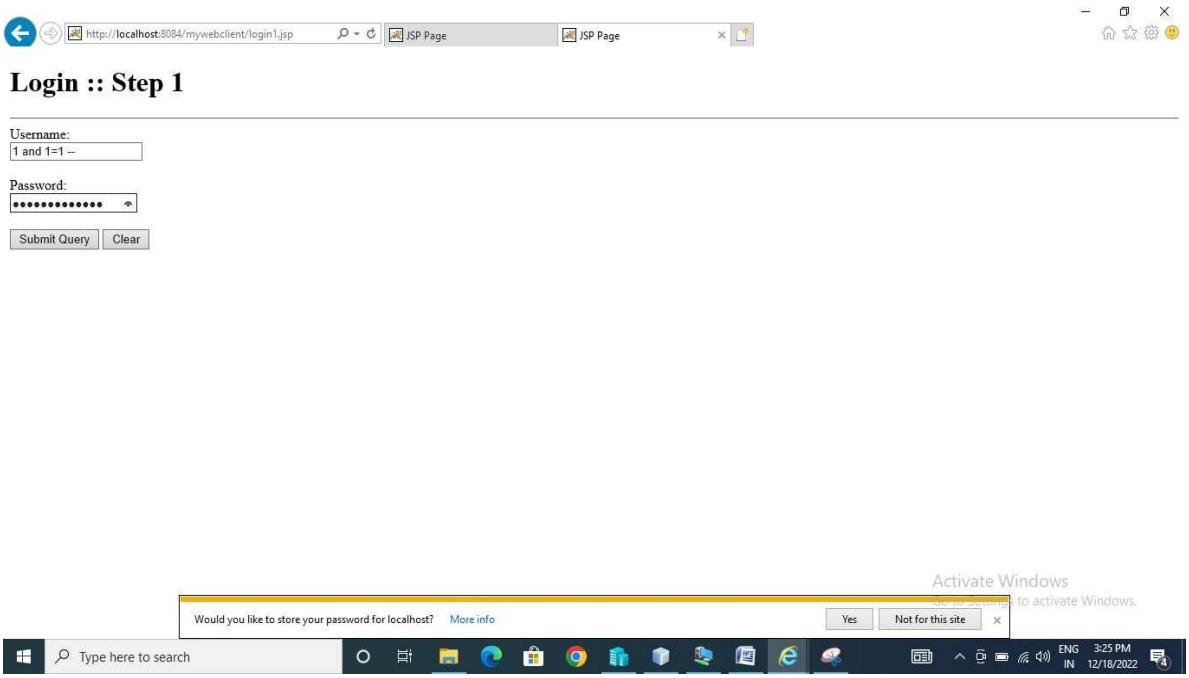

Figure 3.

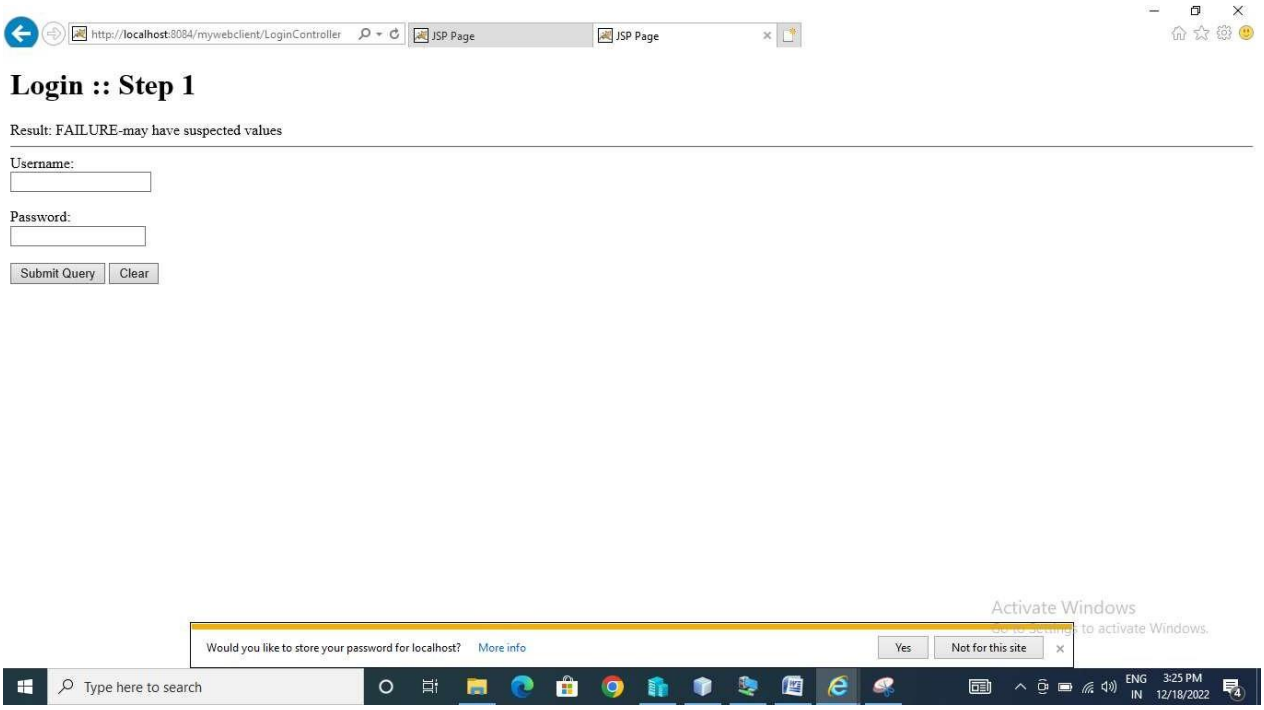

Figure 4.

Similarly figure 5 show the practice of attack and figure 6 exemplify the breakdown endeavor.

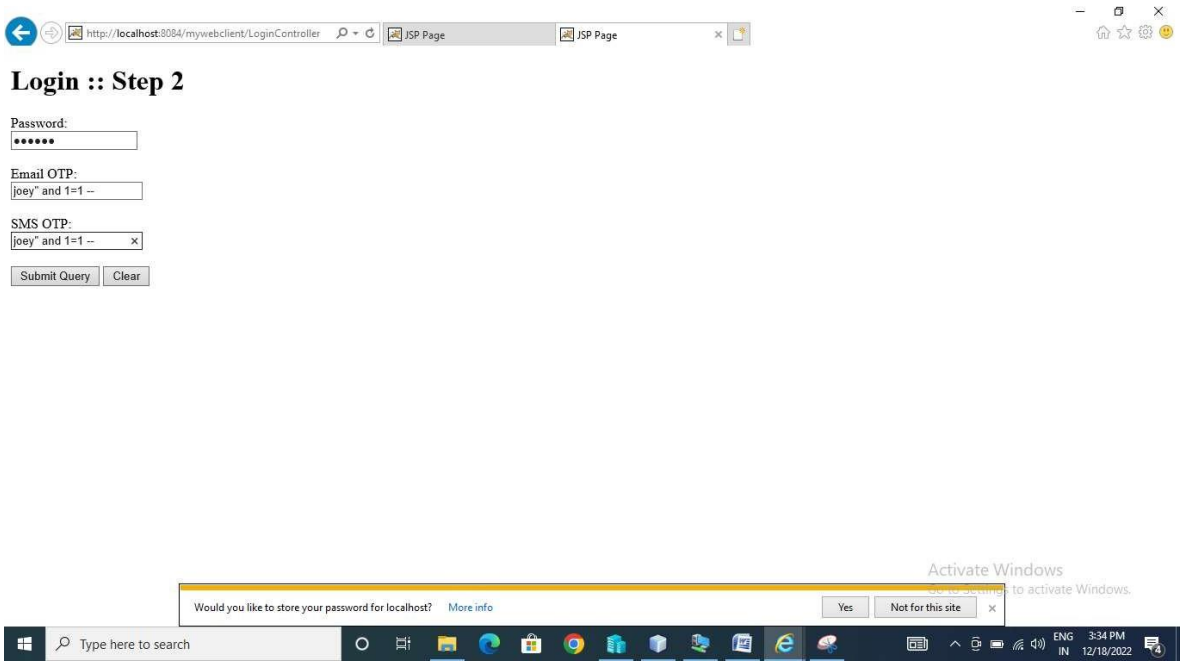

Figure 5.

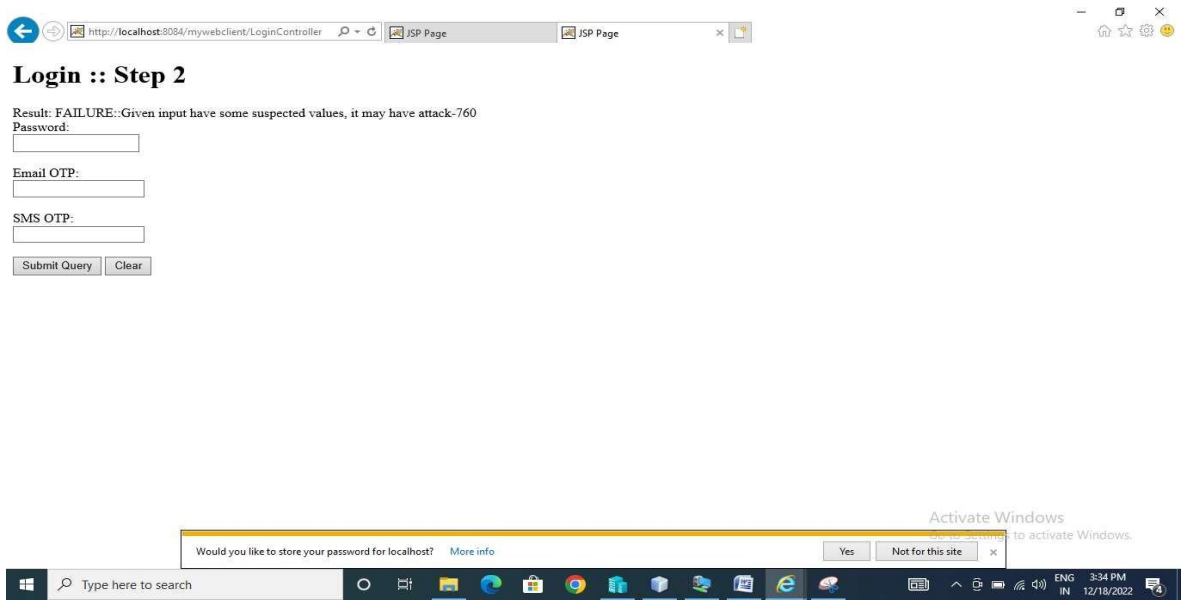

Figure 6.

CONCLUSION

The study impart the obligation of intrusion detection system with authentication system. Additionally proposed paradigm integrates the authentication framework and IDS at the cloud layer above the compute layer to identify the attack before it could manipulate its activity traces as normal. The K-base enriched with mentioned attack patterns from the malicious payloads.The distinguishing feature of the proposed work from its counterpart's is creation of an indigenous database of intrusion activities instead of standard data sets. Simulation practices of multiple cracking tasks demonstrate the applicability of the approach. The strategy detects suspicious activities during the authentication phase to prevent the authentication phase attacks at the cloud layer.

Reference

[1] X. Wang, Z. Yan, R. Zhang, and P. Zhang, "Attacks and defenses in user authentication systems: A survey," *J. Netw. Comput. Appl.*, vol. 188, no. April, p. 103080, 2021, doi: 10.1016/j.jnca.2021.103080.

[2] V. Kumar, S. Jangirala, and M. Ahmad, "An Efficient Mutual Authentication Framework for Healthcare System in Cloud Computing," *J. Med. Syst.*, vol. 42, no. 8, 2018, doi: 10.1007/s10916-018-0987-5.

[3] P. Deshpande, S. C. Sharma, S. K. Peddoju, and S. Junaid, "HIDS: A host based intrusion detection system for cloud computing environment," *Int. J. Syst. Assur. Eng. Manag.*, vol. 9, no. 3, pp. 567–576, 2018, doi: 10.1007/s13198-014-0277-7.

[4] P. Ghosh, A. Karmakar, J. Sharma, and S. Phadikar, *CS-PSO based intrusion detection system in cloud environment*, vol. 755. Springer Singapore, 2019.

[5] W. Elmasry, A. Akbulut, and A. H. Zaim, "A Design of an Integrated Cloud-based Intrusion Detection System with Third Party Cloud Service," *Open Comput. Sci.*, vol. 11, no. 1, pp. 365–379, 2021, doi: 10.1515/comp-2020-0214.

[6] A. Drewek-Ossowicka, M. Pietrołaj, and J. Rumiński, "A survey of neural networks usage for intrusion detection systems," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 1, pp. 497–514, 2021, doi: 10.1007/s12652-020-02014-x.

[7] A. A. R. Melvin *et al.*, "Dynamic malware attack dataset leveraging virtual machine monitor audit data for the detection of intrusions in cloud," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 4, pp. 1–19, 2022, doi: 10.1002/ett.4287.

[8] S. kaur, G. kaur, and M. Shabaz, "A Secure Two-Factor Authentication Framework in Cloud Computing," *Secur. Commun. Networks*, vol. 2022, pp. 1–9, 2022, [Online]. Available: https://www.hindawi.com/journals/scn/2022/7540891/.

[9] V. Balamurugan and R. Saravanan, "Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation," *Cluster Comput.*, vol. 22, pp. 13027–13039, Nov. 2019, doi: 10.1007/s10586-017-1187-7.

[10] A. Meryem and B. EL Ouahidi, "Hybrid intrusion detection system using machine learning," *Netw. Secur.*, vol. 2020, no. 5, pp. 8–19, 2020, doi: 10.1016/S1353-4858(20)30056-8.

[11] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, 2019, doi: 10.1186/s42400-019-0038-7.

[12] I. Studnia, E. Alata, V. Nicomette, M. Kaâniche, and Y. Laarouchi, "A language-based intrusion detection approach for automotive embedded networks," *Int. J. Embed. Syst.*, vol. 10, no. 1, pp. 1–12, 2018, doi: 10.1504/IJES.2018.089430.

[13] Z. Siddiqui, O. Tayan, and M. Khurram Khan, "Security analysis of smartphone and cloud computing authentication frameworks and protocols," *IEEE Access*, vol. 6, pp. 34527–34542, 2018, doi: 10.1109/ACCESS.2018.2845299.

[14] N. Krishnan and A. Salim, "Machine Learning Based Intrusion Detection for Virtualized Infrastructures," *2018 Int. CET Conf. Control. Commun. Comput. IC4 2018*, pp. 366–371, 2018, doi: 10.1109/CETIC4.2018.8530912.

[15] A. Thakkar and R. Lohiya, "A Review of the Advancement in Intrusion Detection Datasets," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 636–645, 2020, doi: 10.1016/j.procs.2020.03.330.

[16] S. More, M. Matthews, A. Joshi, and T. Finin, "A knowledge-based approach to intrusion detection modeling," *Proc. - IEEE CS Secur. Priv. Work. SPW 2012*, no. September 2014, pp. 75–81, 2012, doi: 10.1109/SPW.2012.26.

[17] https://qatestlab.com/resources/knowledge-center/attacks-on-unprotected-login-forms.

[18] https://www.kaggle.com/datasets/syedsaqlainhussain/cross-site-scripting-xss-dataset-for-deep-learning.

[19] https://www.imperva.com/learn/application-security/sql-injection-sqli/

[20] https://www.uptycs.com/blog/intrusion-detection-in-cloud-computing.