International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

A CLOUD-BASED INVASION DETECTION SYSTEM THAT USES SECURE HASHING METHODS

Devendra Babu Kondragunta[1], Dr. T. Judgi[2]

Dept. Of Computer Science Engineering (B.E.) Sathyabama Institute of Science and Technology

---

Abstract - All industries have the same fundamental problem of insufficient defense, but today's adversaries are making significant efforts to penetrate these defenses in order to engage in illegal insider trading. They identify a wide variety of information theft conduits. Private details is more vulnerable to intrusion in the modern world. While there are numerous defenses against various forms of assault, hackers are always developing novel methods of breaching existing defenses. As a result, in this article, we attempted to create a novel approach that would be very resistant to such an assault. The suggested scheme includes the implementation of a hash map-based system for detecting intrusions. In this system, the item is hashed and then stored as a shared key.

The safe transfer of data is a key issue nowadays. Users in the data-sharing system may encrypt their files using their own personal keys before uploading them. If a user leaks the key information, it becomes tough for the cloud provider maintain stay secure, making this attribute extremely crucial to any large-scale data sharing system. In this work, we provide a secure and efficient implementation of the technique, as well as a proof of its security. Many obstacles stand in the way of data owners when they want to make their data available through server or cloud storage. The issues may be addressed in a variety of ways. For the safe management of a shared key belonging to the data's owner, several methods are required. In this article, we'll discuss the concept of a trusted authority as a means of verifying the identities of cloud data users. The trusted authority will utilize the SHA algorithm to produce the key, and then distribute it to the user and the owner. To determine the hash value, the certified authority system utilizes the MD-5 method after receiving an AES-encrypted file from the data owner. It maintains a database with keys that may be accessed during dynamic operations and utilized to identify any cheaters inside the network (CSP or Owner). The CSP module stores files sent from the trusted authority in the cloud. It is shown that the generated key sets have many desired qualities that protect reliable communication from being snooped on by other the network's nodes.

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

1.INTRODUCTION

Cloud-based intrusion detection systems (IDSs) that use secure hashing algorithms are one method of monitoring a network for hostile activities. The system would run on the cloud-based computing platform, that provides flexibility & memory adaptability. To generate a unique digital fingerprint, or "hash," of internet traffic, secure hash functions like SHA-256 & SHA-512 are utilized. The validity of the traffic may be determined by comparing the hash to a known database of good & bad hashes. Cloud computing enables the IDS to store its database of positive and negative hashes and handle massive volumes of data. It also enables remote access, which is useful for both updating and maintaining the system.

The IDS would keep an eye on every data passing across the network and raise an alarm if anything fishy was seen. This has the potential to thwart a broad variety of malicious cyber activity, such as virus infections, malware, and attempted break-ins. All things considered, a combination of cloud computing and secure hashing algorithms in an IDS may be a powerful tool for spotting and stopping network intrusions. The use of secure hash functions in an IDS has several benefits, one of which is that them are very difficult to edit or tamper with. The hash of the network activity an attacker generates will be unusual from the hashing of regular traffic, therefore it will be simple to identify even if they manage to circumvent the IDS.

IDSs that make use of cloud computing also have the option of incorporating machine learning algorithms into their detection processes, further enhancing their precision. To better identify emerging threats, the IDS may, for instance, utilize past information to train a ml algorithm to spot patterns of malicious behavior. One other perk of adopting a cloud-based IDS is its compatibility with other security measures. This includes intrusion prevention systems, firewalls, and antivirus programs. As a result, network security may be tackled in a more holistic and unified manner. Protecting the confidentiality and integrity of your data while employing a cloud-based IDS seems to be a significant problem. It is possible to prevent data theft or manipulation by using encryption and other protection measures. Using cloud computing to deploy an IDS built on safe hashing methods may be a challenging task that necessitates expertise in information security, cloud services, & secured hash functions. Organizations should collaborate with seasoned security specialists to design, build, and manage the system. Understanding the difficulties and complications of deploying an IDS based on safe hashing algorithms utilizing cloud computing is essential for making the most of its potential to identify and deter malicious behavior on a network.

Increased cyber-attacks have been a growing cause for worry as Internet technology has advanced rapidly in recent years. One method for spotting these intrusions is the Intrusion Detection System (IDS). Despite the impressive results of the already available Intrusion Detection techniques, there is a growing need to either refine the existing approaches or create whole new ones. IDSs have been used for a long time with the intention of scanning network traffic and identifying any malicious activity or threats in real time. Just like a firewall, an IDS is a security system whose primary function is to prevent unauthorized individuals from gaining access to sensitive information by ensuring the data's integrity and availability. There are established criteria by which the effectiveness of an IDS may be evaluated.

Accuracy, low resource use, high efficiency, swiftness, and fullness are all in this category. Two types of attack detection techniques are used by IDS: anomaly detection and signature detection (also known as misuse detection). One uses the former to examine system behavior over time to spot out of the ordinary actions taken by the system; for instance, if the number of database queries made by users is much higher than average, an anomaly detection warning will be triggered. As not every user should be treated equally, this is obviously a drawback as well. In the same vein, the number of queries you run every day won't always be the same, thus it's best to make that number variable. The difficulty of adapting anomaly detection to an environment where user needs are constantly changing and cannot be compared to past data is another potential drawback. Therefore, it follows that anomaly detection may produce false positives. In the latter way, rules are built within the IDS based on stored information called fingerprints or signatures of previously successful attacks.

2. LITERATURE REVIEW

Scholars have spent a lot of time thinking about and writing about security intrusion detection systems. The methods used for IDS may be broken down into three broad classes: anomaly-based IDS, letter IDS, and evolutionary algorithms. As a first step in working with massive data sets, dataset pretreatment is essential when dealing with IDS. Choosing relevant features is the primary step in preprocessing. After settling on a set of characteristics, methods of machine learning are used to categorize intruders' typical and atypical activities. We first discuss the hybrid approaches to ml utilized in the IDS there in current work, then we describe the different types of IDS, and last, we describe the method for selecting features.

A. IDs based on Anomaly

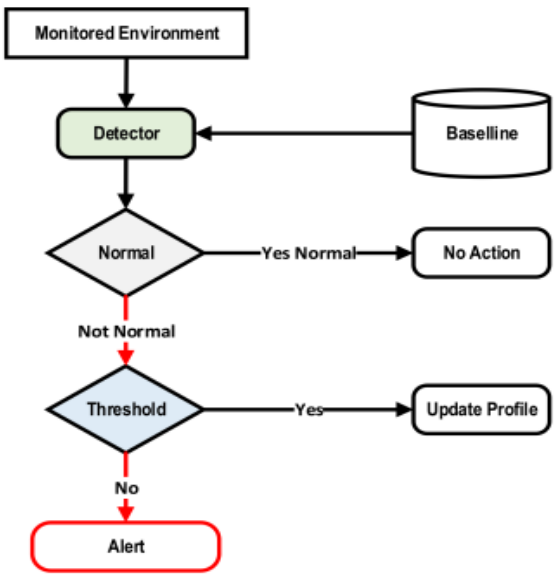

Fig.1. Structure for intrusion detection systems based on anomalies [13]

An advanced optimization approach was presented by Aljawarnehh [14] for intrusion detection systems (IDSs) based around intrusion detection with image segmentation. This novel hybrid model helped estimate assaults based on the activity with processing of best-case training data possibilities. Developing a more accurate IDS model needed additional optimization methods.

By observing patterns in constants (e.g., the amount for the user ought to be the same when logging in), a profiling of a web - based application was created (see to [15] for more details). The software was examined to see whether any of the constants had been broken. There was recorded as an anomaly each time a violation of a static element was noted.

By examining the activity of all online sessions, the authors of reference [16] were able to create an anomaly-based intrusion detection system. It was made up of more manageable data item groupings for companies. These categories were then applied to common patterns in data access utilized in workflow procedures. The authors used a program called a HMM. Evidence was shown that the clustering could achieve low for it for while keeping its accuracy results, and the findings demonstrated that the approach could identify abnormal web transactions.

Double framework was created by Le et al. [17] to identify attacks that released information by checking both database and web server logs. For dynamic sites, they found an FP rate of 0.6% and for static pages, an FP rate of 0%.

In their research, Nascimentto&Correia [18] examined an IDS that had been trained using data gathered from a large-scale online application. They only thought about GET requests and ignored POST requests and their corresponding answer pages. They used the T-Shark log converter to standardize the logs it generated. In order to generate the filtered data, we needed to call upon the ancillary programs. Nine different sensing models were employed.

Ariuu [19] created an HMM-based host-based IDS to prevent attacks on mobile apps. A web application's input properties and values were modelled using this technique. Multiple HMMs were concatenated in order to meet a certain requirement on the probabilities that was derived from the training sample, allowing for the calculation of various metrics and values.

Using a "XML" file that provided the necessary properties of parameter values, a web-based firewall was created in reference [20] to identify any irregular requests and record their behaviors. Attacks were detected if input values strayed from the profile. The problem was that this method generated FP warnings since it ignored the more reliable route information and page.

A. IDS systems that rely on signatures based on previously detected threats are better able to spot new threats as they emerge. The network interface layout is compared using this method. When an attack occurs and the network interface pattern fits the signature, the entry is flagged. By understanding the network behavior fingerprints, this sort of detection scheme is simple to create and comprehend. This method detects

known assaults with a high degree of accuracy and almost no false positives. Additionally, it may replenish the database with new signature and affecting the pre-existing ones. The biggest problem with this IDS method is that it may be fooled by even the slightest change in the attack pattern, therefore it won't be able to prevent assaults that haven't been seen before. Schematic representation of signature-based IDS architecture. Here are some relevant works that have used biometrics IDS.

B. IDs based on signatures

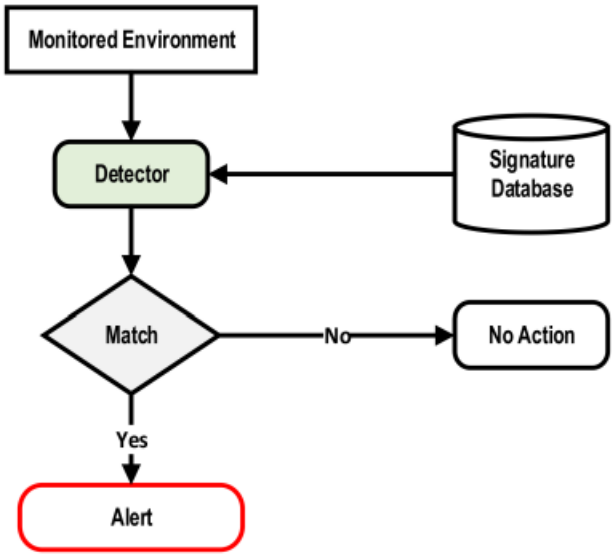

Fig.2. Architecture for intrusion detection systems based on signatures [13]

IDS systems that rely on signatures based on previously detected threats are better able to spot new threats as they emerge. The network interface layout is compared using this method. When an attack occurs and the network interface pattern fits the signature, the entry is flagged. By understanding the network behavior fingerprints, this sort of detection scheme is simple to create and comprehend. This method detects known assaults with a high degree of accuracy and almost no false positives. Additionally, it may replenish the database with new signature and affecting the pre-existing ones. The biggest problem with this IDS method is that it may be fooled by even the slightest change in the attack pattern, therefore it won't be able to prevent assaults that haven't been seen before. Schematic representation of signature-based IDS architecture. Here are some relevant works that have used biometrics IDS.

Saraniyaa [21] created an IDS algorithm that relies on signatures to identify network intrusions, and this system is called a NIDS. It was able to successfully collect packets from the whole network in wide range of operating conditions and compare them to attack patterns created by security experts. As a result, the network was protected and memory use was cut down.

Because of trademark library has to be constantly examined for every fresh kind of intrusion found, biometrics IDS cannot identify new and undiscovered threats. Cyberattacks against MODBUS-based industrial control systems and signature-based intrusion detection systems were the subject of research presented by Gao and Morris [22]. The assaults discussed before were the inspiration for the regulations mentioned. The regulations were classified as either "unbiased" or "legislature." Rules that examined a single MODBUS package for a matching sign were totally independent. Snort, an ids, enforced the isolated rules.

Uddinn[23] presented a new operator for signature-based networked IDS, which would move signatures from a big complimentary warehouse to a small data store, and then frequently update the libraries when new signings were identified. The suggested model's findings shown that IDS outperformed conventional systems that relied on a central database of chain fingerprints.

In [24], Kumar and Gobil built an IDS that relies on previously-created signatures. They created an intrusion detection system (IDS) using Chortle, Basis, & Tp Rewind. This technology has the potential to analyze network traffic in real-time for signs of infiltration.

3. PROPOSED SYSTEM

An organization's unique requirements and available resources will determine which of many suggested systems for an IDS based on secure hashing algorithms in the cloud would be the best fit. Nevertheless, the following are some things that should be considered while designing the ideal system:

1) Using secure hashing algorithms like SHA-256 and SHA-512, which are widely used in business, to guarantee the legitimacy of data sent across a network.
2) Using cloud computing as the foundation allows for scalability and the capacity to manage massive volumes of data.
3) Machine learning techniques are used to enhance the system's detection capabilities and respond more rapidly to emerging threats.
4) For a more unified and effective network security strategy, integration with other security tools and services like firewalls, antivirus software, and intrusion prevention systems is essential.
5) Taking precautions to safeguard information stored in the cloud, such as using encryption and other safety protocols.
6) A user interface that is both straightforward and instinctive, facilitating IDS management and monitoring by system administrators in real time.
7) Updating and maintaining the system on a regular basis is essential for keeping it secure against new forms of cyberattack.
8) The capacity to meet regulatory requirements, such as PCI-DSS, HIPAA, and ISO 27001.

9) Planned actions to take in the event of a breach, should one occur.

To solve the problem of insecure digital certificates and data sharing in dynamic groups, we present a new secure data sharing technique. We provide a safe method of key distribution that doesn't need any private lines of communication. Users' public keys may be verified by the group manager, allowing them to safely get their private keys without the need for Certificate Authorities. With the aid of the

group's user list, our approach is able to establish granular control over who has access to which parts of the data. We provide a safe way of exchanging information that is immune to collusion. Once a user's access has been denied, even if they operate together with an untrusted network, they will not be able to retrieve the original data files. The usage of a polynomial function allows our system to provide safe user revocation.

Our approach quickly supports dynamic group, meaning that the security tokens of all the other individuals don't need to be theoretical and updated whenever a new customer participates in the club or an existing user is removed from the company. Detection accuracy is provided to demonstrate the safety of our approach.

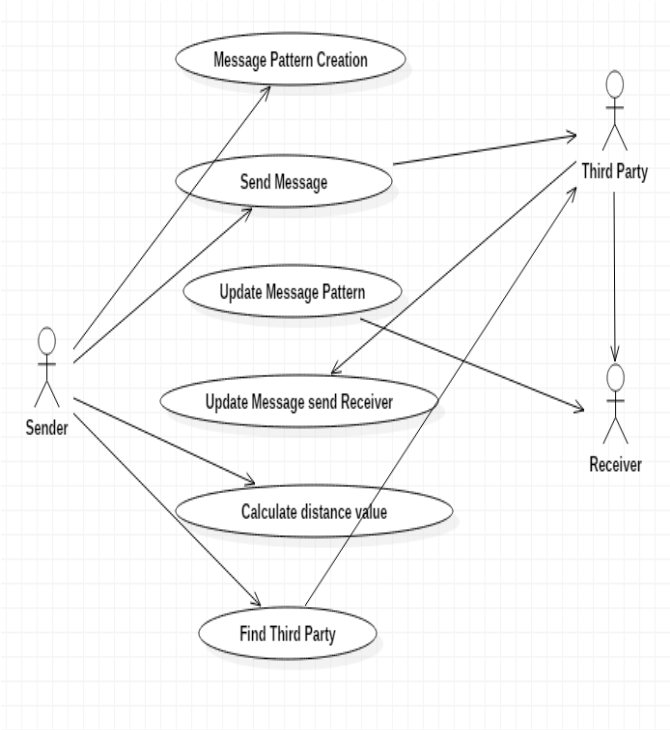

Fig.3. Framework for the application's procedure.

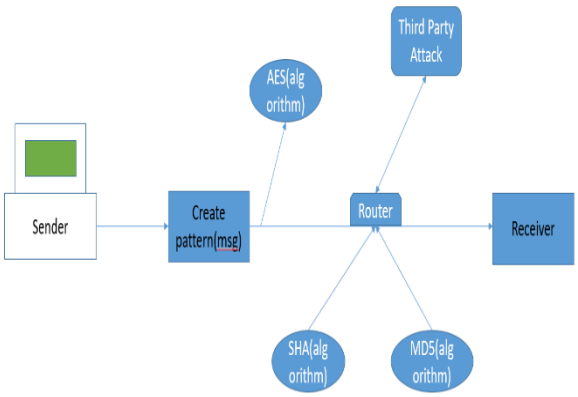

Fig.4. System's Architecture.

4. METHODOLOGY

Intrusion detection systems (IDS) built on the premise of cloud computing and secure hashing algorithms may use the following approach and course of action.

1) The first stage is to gather data on network traffic for use in the IDS. A networking sniffer or even other network management tool might be used to acquire this information.
2) Next, a secure hashing technique, such SHA-256 or SHA-512, would be used to the acquired network traffic data to produce a one-of-a-kind hash.
3) This would involve building a database of trusted and unsafe hashes. Standard network traffic would be used to produce the good hashes, while malicious network traffic would be used to produce the bad hashes.
4) The IDS would next do an analysis of the internet activity by comparing the traffic's hashes to those stored in the database. The intrusion detection system (IDS) will sound an alarm if the traffic's hash corresponds to a previously identified malicious hash.
5) Assembling the IDS in the cloud is the plan. In terms of storage and resources, this provides for scalability. Additionally, remote access is made possible.
6) It is possible to increase the system's precision with the use of machine learning algorithms by analyzing network data for indicators of malicious behaviors. A machine learning model may be trained using data from the past, allowing the system to identify new threats more rapidly and correctly.
7) Data stored in the cloud would be shielded from prying eyes and unauthorized access with the help of encryption and other security measures.
8) Updating and Repairing: The system would be checked and repaired on a regular basis to make sure it is always working well and can identify and avoid any new cyber threats.

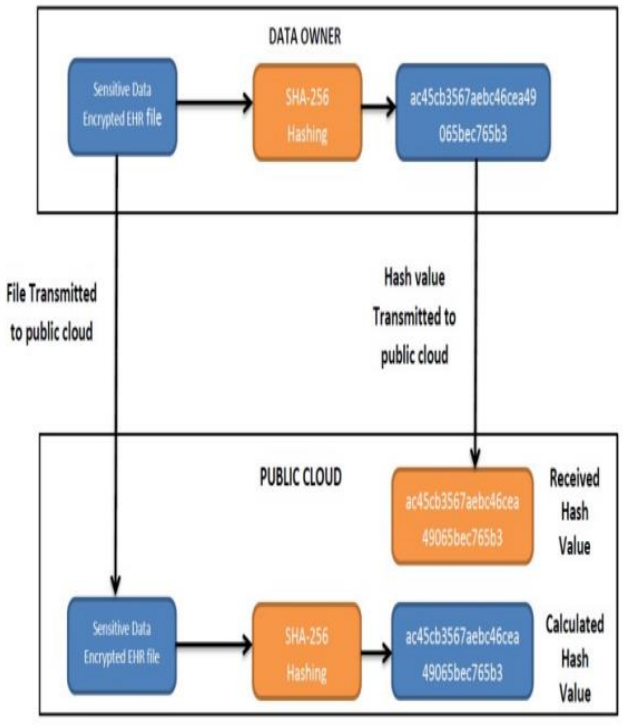

Fig.5. Protocol for ensuring data integrity during transmission from data holder to cloud platform.

collecting and analyzing network traffic data, building a collection of known good and bad hashes, deploying the IDS on a cloud platform, integrating ml algorithms for greater accuracy, and enforcing security precautions to safeguard data stored in the cloud are all components of the proposed method for an IDS based on secure md5 techniques using cloud storage.

5. EXPERIMENTAL RESULTS

In this part, we give the results of the tests performed to assess the performance of the various signature hashed methods presented in the previous section. An important purpose of many algorithms is to prevent hackers from accessing sensitive information that has been generated. Attacks designed to break encryption techniques have proliferated in tandem with their development. These attacks may be thwarted in a number of ways, one of which is by adopting a more modern security protocol or updating the one already in use. Some assaults were successful in breaching the security given by SHA -1 Algorithms, diminishing its promise for data privacy. Therefore, Privacy was not successfully protected by SHA-1. For increased safety, SHA 2 was created by NSA experts.

Fig.6. Values hashed out by several algorithms and compared.

A variety of theoretical attacks aimed at breaking SHA 2's security were explored. However, while SHA 2 is more secure than SHA 1, there is no assurance that any private information will be leaked. SHA-2 makes attacks such as the Overlap Attack and the Pre-Image Attack vulnerable.

In a collision attack, the attacker seeks to discover inputs that will result in the same hash value for the output. Collision attacks may be divided into two categories. Since SHA-2 uses a six-value digest, this collisions approach is only effective against SHA-1[12], but not against SHA-2's Failsafe mechanism. With SHA-2, it's difficult to encrypt files since any two inputs will generate distinct hash values.

Normal Pre-Image Assault By "Pre-image Attack," we imply an assault that begins with the discovery of an image (fault in code) in a security algorithm, and then proceeds to discover that same picture during a subsequent attack. Because SHA 2 has Attribute based Opposition, it is immune to this kind of attack before it ever begins. This is because SHA 2 employs the double hashing approach, which makes it almost impossible for an attacker to create a valid preimage. SHA-256 is not vulnerable to Hash Collision, a situation in which attackers generate input data sources for the same hashing values, resulting in the exact same emission hash values. This is in contrast to the MD (1,2,3,4,5) Clustering Method as well as the SHA-1 Hashing Method.

6. CONCLUSIONS

When combined with other forms of security, such firewalls, an IDS may greatly improve the effectiveness of a network's defenses. The primary function of an IDS is to spot the telltale symptoms of an attack, notify the system administrators, and have them relay fake information to the intruders. IDS are often divided into two distinct types, based on their approach to detection: exploitation identification & outlier detection. In terms of how they function, you may place them in either the network or host category of intrusion detection systems.

Today's IDS include data gathered from both the network and the host computer. The more threats an Intrusion Detection System finds and sends to the false data to hackers, the more convincing it seems to be. Hence By encrypting the secret message by hash but moreover if the developer split seem to be hash code it will get just the false info, OTP will similarly would now there for confirmation, we are trying to overcome the disadvantage of the current system. it provides an integrated home that will not only be control and monitor our data with segregation of duties but also prevent malicious attacks.

REFERENCES

[1] 1. Medical Data in the Crosshairs: Why Is Healthcare an Ideal Target? 14 August 2021. Available online: https://www.trendmicro. com/vinfo/us/security/news/cyber-attacks/medical-data-in-the-crosshairs-why-is-healthcare-an-ideal-target (accessed on 15 May 2020).

[2] Conaty-Buck, S. Cybersecurity and healthcare records. Am. Nurse Today 2017, 12, 62–64.

[3] eGOVERNMENT, Cloud Computing Initiatives. 22 April 2021. Available online: https://www.bahrain.bh/ (accessed on 15 July 2021).

[4] Moukhafi, M.; El Yassini, K.; Bri, S. A novel hybrid GA and SVM with PSO feature selection for intrusion detection system. Int. J. Adv. Sci. Res. Eng. 2018, 4, 129–134.

[5] Kuang, F.; Xu, W.; Zhang, S. A novel hybrid KPCA and SVM with GA model for intrusion detection. Appl. Soft Comput. J. 2014, 18, 178–184.

[6] Al-Yaseen, W.L.; Othman, Z.A.; Nazri, M.Z.A. Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system. Expert Syst. Appl. 2017, 67, 296–303.

[7] Feng, W.; Zhang, Q.; Hu, G.; Huang, J.X. Mining network data for intrusion detection through combining SVMs with ant colony networks. Future Gener. Comput. Syst. 2014, 37, 127–140.

[8] Ambusaidi, M.A.; He, X.; Nanda, P.; Tan, Z. Building an intrusion detection system using a filter-based feature selection algorithm. IEEE Trans. Comput. 2016, 65, 2986–2998.

[9] Mustapha, B.; Salah, E.H.; Mohamed, I. A two-stage classifier approach using RepTree algorithm for network intrusion detection. Int. J. Adv. Comput. Sci. Appl. (IJACSA) 2017, 8, 389–394.

[10] Tuan, A.; McLernon, D.; Mhamdi, L.; Zaidi, S.A.R.; Ghogho, M. Intrusion Detection in SDN-Based Networks: Deep Recurrent Neural Network Approach. In Advanced Sciences and Technologies for Security Applications; Springer: Berlin/Heidelberg, Germany, 2019; pp. 175–195.

[11] Nguyen, K.K.; Hoang, D.T.; Niyato, D.; Wang, P.; Nguyen, D.; Dutkiewicz, E. Cyberattack detection in mobile cloud computing: A deep learning approach. In Proceedings of the IEEE Wireless Communications and Networking Conference, Barcelona, Spain, 15–18 April 2018.

[12] He, D.; Qiao, Q.; Gao, Y.; Zheng, J.; Chan, S.; Li, J.; Guizani, N. Intrusion detection based on stacked autoencoder for connected healthcare systems. IEEE Netw. 2019, 33, 64–69.

[13] Mudzingwa, D.; Agrawal, R. A study of methodologies used in intrusion detection and prevention systems (IDPS). In Proceedings of the IEEE Southeastcon, Orlando, FL, USA, 15–18 March 2012.

[14] Aljawarneh, S.; Aldwairi, M.; Yassein, M.B. Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. J. Comput. Sci. 2018, 25, 152–160.

[15] Ludinard, R.; Totel, É.; Tronel, F.; Nicomette, V.; Kaâniche, M.; Alata, É.; Bachy, Y. Detecting attacks against data in web applications. In Proceedings of the 7th International Conference on Risks and Security of Internet and Systems (CRiSIS), Cork, Ireland, 10–12 October 2012.

[16] Li, X.; Xue, Y.; Malin, B. Detecting anomalous user behaviors in workflow-driven web applications. In Proceedings of the IEEE Symposium on Reliable Distributed Systems, Irvine, CA, USA, 8–11 October 2012; pp. 1–10.

[17] Le, M.; Stavrou, A.; Kang, B.B. DoubleGuard: Detecting intrusions in multitier web applications. IEEE Trans. Dependable Secure. Comput. 2012, 9, 512–525.

[18] Nascimento, G.; Correia, M. Anomaly-based intrusion detection in software as a service. In Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W), Hong Kong, China, 27–30 June 2011; pp. 19–24.

[19] Ariu, D. Host and Network Based Anomaly Detectors for HTTP Attacks. Ph.D. Thesis, University of Cagliari, Cagliari, Italy, 2010.

[20] Gimenez, C.; Villaegas, A.; Alvarez, G. An Anomaly-Based Approach for Intrusion Detection in Web Traffic. J. Inf. Assur. Secure. 2010, 5, 446–454.

[21] Saraniya, G. Securing the Network Using Signature Based IDS in Network IDS. Shodhshauryam Int. Sci. Refereed Res. J. 2019, 2, 99–101.

[22] Gao, W.; Morris, T. On Cyber Attacks and Signature Based Intrusion Detection for Modbus Based Industrial Control Systems. J. Digit. Forensics Secure. Law 2014, 9, 37–56.

[23] Uddin, M.; Rehman, A.A.; Uddin, N.; Memon, J.; Alsaqour, R.; Kazi, S. Signature-based multi-layer distributed intrusion detection system using mobile agents. Int. J. Netw. Secure. 2013, 15, 97–105.

[24] Kumar, U.; Gohil, B.N. A Survey on Intrusion Detection Systems for Cloud Computing Environment. Int. J. Compute. Appl. 2015, 109, 6–15.