ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

Software Attack Detection and Prevention Using Machine Learning Algorithms in Cloud Computing

Mrs. Archana Paike, Mrs. Sayali Ambavane, Mrs. Megha Yawalkar

Department of Computer Engineering, Government Polytechnic, Pune, Maharashtra, India

ABSTRACT: Software-as-a-service (SaaS) is a methodology for delivering software services that covers a wide variety of business possibilities and constraints. Users and service providers are hesitant to incorporate their businesses into SaaS because of security concerns, even if the advantages are appealing. The usefulness and application of SaaS in various situations such as cloud computing, mobile cloud computing, software defined networking, and the Internet of Things are highlighted in this article. The report then goes on to examine SaaS security issues such as data security, application security, and SaaS deployment security, as well as various solutions or strategies that may be used in combination to create a safe SaaS platform. The goal of this study is to find harmful activities in the cloud-based Software as a Service (SaaS) environment. Cloud forensics is the process of investigating cybercrime in the cloud environment in a forensically sound way, in addition to investigating crimes connected to the cloud environment in a forensically sound manner. Because of the dynamic nature of cloud computing, this procedure is fraught with difficulties. It also proposes a cloud forensic technique to aid digital investigators and specialists in conducting successful and efficient cybercrime investigations. The suggested solution relies on a cloud computing infrastructure with massive processing and storage capacity. This technique may serve as a guide for digital investigators and practitioners while conducting SaaS attack investigations.

KEYWORDS: Virtual Machine, Digital, Provenance, Isolating Cloud Instance, Regeneration of events, Regeneration of events.

I. INTRODUCTION

Cloud technology is changing, and cloud-based storage is a new word that not only makes it simpler for users to upload data to the internet, but also enables them to have instant access to relevant resources and share data with others at any time. However, since cloud-based information may be accessed anywhere, on any device, and very few indicators are left about, cloud-based information creates a difficulty for the person who investigates and identifies forensic material that might aid in forensic inquiry.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

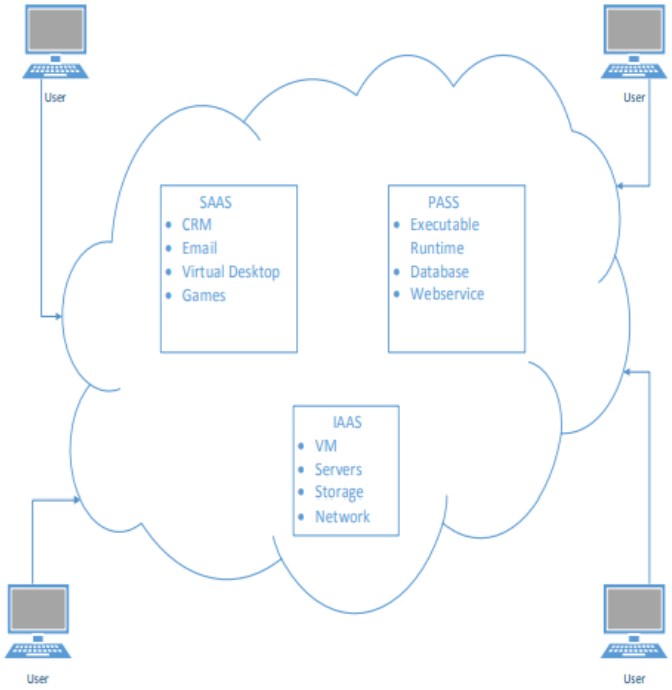

Figure 1 Current Cloud defense mechanism Scenario

The twenty-first century is known as the digital era. There would be a significant introduction of machines. Today, we couldn't survive without computers and the Internet since we depend on them for practically all of our tasks. Everything has subsequently been automated into computers, from home to job to banking and even corporate business. All of our key data is filtered in the digital format. As shown in Figure 1: Existing Cloud Scenario, the requirement to store digital data has grown, and the virtual world has overtaken physical storage to hold all of our certifications. The most dangerous difficulty in the cloud is preventing illegal deletion of stored cloud data, since you may quickly remove items without necessary authority. The deletion of data is totally reliant on the deletion of nodes that refer to virtual machine information.

Various distributed computing expert co-ops and their administrations are accessible in the cloud. For achieving security, these presidencies combine various judgments, illustrations, and technology. Some presidencies concentrate on secure access to administration and critical data through encrypted data, while others concentrate on the secure server itself. The procedures used by different providers to ensure protection are always changing. A cloud client may search for an administration depending on the administration's requirements and security level. A test is used to deconstruct a certain administration by looking at its many security features. In terms of security, trusting a cloud management or expert organisation is the ultimate test. One might strive to exhibit such "confidence" in an administration as a kind of confidence esteem. This theory investigates a system's probability, such as a confidence computing process, and its different characteristics.

II. LITERATURE REVIEW

So far, a critical review of the work on Cloud Forensics has been conducted to explain how the new research applies to what has already been conducted. Because of greater economic challenges, several businesses are now migrating to the cloud for a few days. But for small and medium-sized businesses, the primary concern is information security. The best choice for these businesses is to use a managed service, also known as an outsourced service, in which the entire service bundle, including antivirus software, is delivered for security consulting. And Security as a service (SECaaS) is the alternative model that provides such outsourced security. Together, scientists and researchers discussed their new ideas

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

and observations about what the real world scenario is and what all attempts are being undertaken, but it was found that there is just a fraction of the overall work that has contributed to the wealth of society despite being so much research work in the field of cloud forensics. Cloud, though, came into being in the mid-90s, but it is not completely taken up by anyone. There has been a lot of work in this area before and a number of techniques for cloud forensic analysis, but there is a significant space for progress that needs to be carried further in the study.The VM forensic investigation technique uses snapshots as evidence that can be shown before the court of law as proof. The software stored and maintained snapshots of the running VM selected by the user in that mechanism, which acted as good evidence. The user can build VMs from the physical machines available, according to his preference. Any cloud software similar to that of Eucalyptus instead of request of a user, takes the snapshots of the machines stores till terminated. Snapshots can only be stored until the maximum is reached, but the snapshots that were taken long before being deleted are reached when the maximum is reached. The enormous storage management of VM snapshots is therefore difficult as it impacts the system's efficiency.

In recent years, the rapid rise of the Internet of Things (IoT) has resulted in a major increase in fog computing, smart cities, and Industry 4.0, all of which perform complicated data processing of personal information that must be safeguarded from cybersecurity assaults. Various fields, such as smart homes, healthcare, energy, agriculture, automation, and industrial processes, have seen a significant growth in cybersecurity assaults [1]. IoT device sensors create significant volumes of data as a consequence of their broad variety of services, which necessitates authentication, security, and privacy. Traditional methodologies and frameworks were previously employed to assure IoT security. However, in recent years, the use of various artificial intelligence (AI) approaches for identifying cybersecurity breaches has grown in favour. The Internet of Things (IoT) consists of networked devices that are progressively being built on a wide scale, taking into consideration different features through cloud and fog computing, where real-time application processing may be improved [2]. Cyber-physical systems (CPSs) are integrated technologies that are part of the fourth industrial revolution (Industry 4.0) and are used for innovation in smart industries to promote data transmission between networks [3,4]. They include healthcare IoT, industrial IoT (IIoT), smart cities IoT, AI, and big data. Several academics have built IDSs based on different AI techniques to address the security challenges that face the IoT. For example, Kurte et al. [5] proposed a distributed service architecture for developing trustworthiness and privacy protection for multidirectional data aggregation for edge computing improvement [6]. To identify cybersecurity assaults in IoT, Diro and Chilamkurti [7] suggested a detection system based on deep learning (DL) algorithms. They compared the deep learning (DL) model to classic machine learning (ML) methods. Farivar et al. [8] offered a hybrid intelligent classic control strategy for the reconstruction of cyberattacks on the input data of non-linear CPS via shared networks, and identified AI for the detection of malicious assaults in CPS and IIoT. Security in the IoT necessitates extra considerations, such as utilising effective AI approaches to monitor linked smart devices for attacks and other vulnerabilities [9–11]. In addition, AI-enhanced encryption methods are used in IoT security systems to archive privacy [12,13]. Obaidat et al. [14], for example, analysed in-depth IoT attacks, threats, and vulnerabilities using a rating system based on severity impact, as well as a multi-faceted way to address those security problems. Li et al. [15] introduced a security framework based on a homomorphic encryption method over a matrix ring, which also enables ciphertexts homomorphic comparison, as a unique privacy prevention of ML training with classification process. Sarica and Angin [16] proposed a real-time automatic intrusion detection technique in the software-defined networking (SDN) application layer to identify an assault, providing explainable security in IoT networks. Aleem et al. [17] discuss data warehouse (DWH) security risks for each security strategy. If the countermeasure is inadequate, it also contains a new and unique CPS [18]. For safeguarding a virtual machine in cloud computing, Patil et al. [19] suggested a virtual machine-assisted lightweight agent-based malware detection framework, while Dang et al. [20] offered an authentication technique for securing cloud servers in IoT contexts. Moustafa [21] also presented a novel distributed IoT network architecture based on an AI-based security solution. AI approaches are frequently utilised to provide security to IoT devices and networks, owing to its IDSs, in order to overcome obstacles, security concerns, and irregularities [22]. According to Ghosh et al. [23], the use of AI in IoT is a milestone in terms of decreasing human effort in ensuring security. Bland et al. [24] provided more current research, proposing machine learning (ML) offensive and defensive tactics that use reinforcement learning algorithms to increase the capacity to identify cybersecurity threats. Rathore and Park [25] proposed a fog-based attack detection framework and an extreme learning machine (ELM)-based semi-supervised fuzzy method to achieve adequate generalization performance at a fast detection rate using a semi-supervised learning-based distribution attack detection framework for IoT. Kasongo and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

Sun [26] used a DL technique to create a wireless IDS strategy based on wrapper-based feature extraction for wireless networks and a feed-forward deep neural network. However, there are certain restrictions since the use of AI in cybersecurity detection exposes IoT devices and networks to a great deal of risk. Several centralized attack detection systems have been developed to identify assaults in the IoT utilizing a supervised ML algorithm, in addition to the development of IoT. Despite this, due to the unique needs of devices, such as scalability and dispersion, these approaches have failed to provide meaningful outcomes [25]. However, IoT security standards are needed to assess the present approaches [27]. Previous thorough reviews have significantly aided the area of cybersecurity. [28] evaluated and identified the performance of empirical research on techniques to protect IoT environments in order to examine and assess the relevance of artificial immune systems in IoT settings. By formulating and addressing research questions, and filling current research gaps in the area of IoT security by attempting to overcome limitations in the existing work, we hope to explore and analyse both ML and DL methods used for the detection of cybersecurity attacks in IoT devices and networks in this review. For detecting cybersecurity assaults in mobile devices with integrity verification methods for cloud storage in an endpoint context, IDSs, especially those created with AI such as anomaly-based, are favored [2,29–31]. We examine the research on IoT security that has been published and identify the best feasible solutions for various circumstances, including detection algorithms, frameworks, designs, and models. Artificial immune systems have already been investigated for securing IoT through fog orchestration [28,30]. We mapped the literature to discover previous learnings and analyse possible future situations in this paper.

III. METHODOLOGY OF PROPOSED SURVEY

A. Virtual Computer Introspection

It's a smashing virus that monitors and identifies virtual machine risks. When an attack is detected, a Virtual Machine Monitor (VMM) or a VM operating under the VMM evaluates the attacked VM. Garfinkel and Rosenblum were the first to develop this technology, which they named Virtual Machine (VMI) introspection. Malicious events may be recognised via Virtual Machine Introspection, which is a means of analysing a running VM from another VM not under examination or the hypervisor. Live Forensic analysis is also done on the target device using the open-source VMI library and Xen Suite. The most realistic way to detecting the rogue VM is presented as virtual machine introspection. If the intrusion detection system is installed on the host, it may be vulnerable to assault, but if the intrusion prevention system is installed on the network, it is more susceptible to illness. Where the intruder for great attack sensitivity was outside of the device, a soul searching-based virtual machine method to intrusion detection systems was used.

B. Digital Provenance

Digital Provenance is a legal term that refers to an examination into the history of digital objects in the cloud that is admissible in a court of law. The history of a digital item is described by digital provenance, which is a significant element for forensic investigations. Muniswamy and his colleagues introduced the secure provenance approach, which does digital forensics in the cloud using trustworthy evidence. This approach demonstrates that cloud data evidence may be used in court. Researchers identified four qualities that are critical for provenance systems, and methods for storing data provenance via cloud services were developed. Provenance may also be accessed as a layer on top of cloud. The relevance of data on the cloud has grown since safe provenance was implemented.

C. Isolating Cloud Instance

The process of isolating a cloud-related event from a criminal event in order to avoid data abuse and disclosure. When a crime occurs on the cloud, microvasculature and data acquired from various clouds, as well as digital analysis, must be segregated. Seclusion protects the evidence from possible tampering and deterioration. The cloud example's isolation aids in the preservation of the validity of the system gathered from the domain example. Delport and his colleagues have devised new methods for disentangling the cloud services mentioned in our approach.

D. Model Log

The Database Model seems to be something that utilises all of the cloud activities that might be employed for research purposes once again. Dumping is a difficult problem in cloud computing systems, and it is growing more prevalent across all service types. Ting illustrated how forensic specialists can work more efficiently in the cloud if logging

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

capacity is increased, and he proposed a log format that is suitable for SaaS and PaaS. A log may be used internally and sequentially in SaaS to verify the operations on the cloud framework without engaging with the cloud server. It is important to rely on cloud infrastructure that includes a foreign government database module in order to employ the intended log model and PaaS cloud. The suggested log-based solution would solve the cloud behavioural user authentication analytical difficulties..

E. Regeneration of events

By capturing photos of each event in the cloud, it is feasible to renew events. To get digital proof, the most typical way is to capture photographs of the events that have transpired. Snapshots may be obtained in order to recreate a crime scene utilising the time of creation. Belorkar and his colleagues suggested a novel method for recreating crime occurrences using continuous snapshots. For popular cloud services like Eucalyptus, OpenStack also provides a framework for submitting photos of cloud happenings. The honeysuckle walrus screenshots will be saved in the honeysuckle walrus section. It's been pointed out that the picture should be the same size as the original. Though screenshots may be stored in data memory, saving a large number of screenshots for each VM event would be difficult, time-consuming, expensive, and slow. The CSPs might additionally offer a segregation mechanism, as well as mappings for which VMs belong to which snapshots. We propose to resolve this problem with our technique.

F. Forensic Investigation as Evidence using VM Snapshots

Cloud service providers offer a variety of services to users; however, a small number of users from a single organisation often use the same type of service based on pay-per-use, and some providers offer unlimited bandwidth and storage space for free trial periods, giving users the opportunity to engage in malicious activities. Malicious users may steal sensitive and private data from cloud users, jeopardising the CSP's reputation. Cloud has to be protected from these harmful actions, and CSPs should be able to follow client virtual machines and identify malicious behaviour using introspection or intrusion detection methods. Users may construct virtual machines (VMs) from any accessible real computer. Any cloud programme, such as eucalyptus, produces snapshots of a running VM continually, ignoring the user's request, and keeps them until the VM quits. If the maximum number of snapshots for a certain allocated VM is reached when the oldest VM is destroyed, you will store the maximum number of snapshots for that VM. Snapshots in the cloud provide rich sources of evidence for digital investigations and may be used to recreate occurrences. It's tough to save and manage a large number of VM snapshots. Snapshots limit the output of a virtual machine depending on how long they are held and how much they have changed since the last snapshot was taken. Excessive location access, uploading viruses to a variety of network infrastructure systems, extreme amounts of short-term downloads and uploads, introducing complex attack points, cracking encryption, flightcreting web application based servers or variegated tables, corruption or obliteration of complex data, and malevolent activity are all examples of malicious activity. Our proposed approach incorporates a virtual machine intrusion detection architecture that allows it to monitor and detect itself. Cloud suppliers install, operate, and manage the sensor network.

IV. SYSTEM ARCHITECTURE

For element persons, we suggest a secure information sharing approach. Initially, we offer a secure way for key distribution using secure communication channels, and clients may get their private keys from the gathering chief in a secure manner. We employ three separate entities in our proposed system: the data owner, the group manager, the cloud server, and the attacker, who is an untrusted entity. In this module, the data owner uploads the data file to the cloud server using a cryptography method. Once the data is stored in the database, the owner receives information that the file has been successfully stored.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

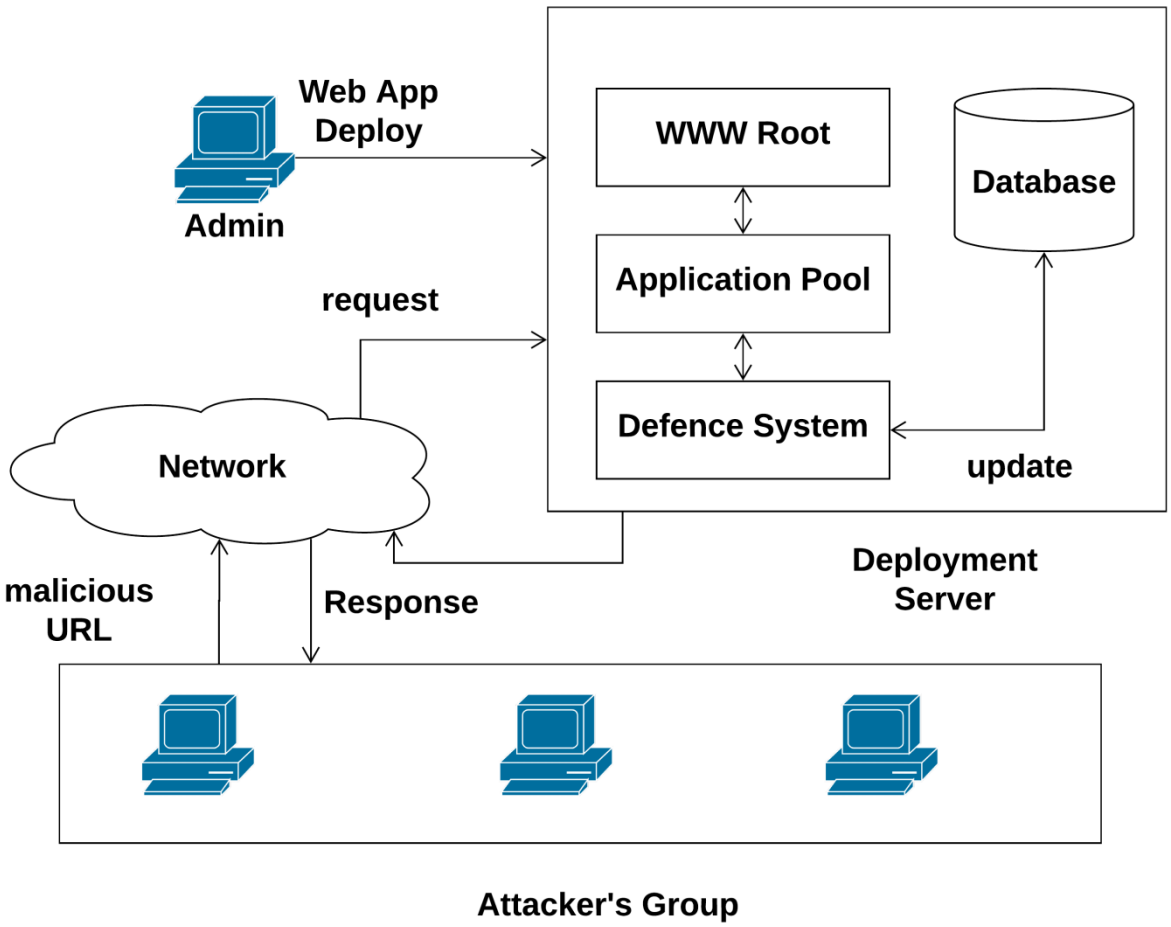

Figure 2 : Propsoed system architecture

For element persons, we suggest a secure information sharing approach. Initially, we offer a secure way for key distribution using secure communication channels, and clients may get their private keys from the gathering chief in a secure manner. We employ three separate entities in our proposed system: the data owner, the group manager, the cloud server, and the attacker, who is an untrusted entity. In this module, the data owner uploads the data file to the cloud server using a cryptography method. Once the data is stored in the database, the owner receives a message that the file has been successfully stored. The data owner has complete access to any data file that he may share or access, therefore the data owner can share any file with any group manager, and it will be accessible to all group members immediately. Members of a shared group may view each file through a cloud server at any time. In the first phase, if the data owner prevents a user from accessing a file, that user is unable to access that file. Even if he is able to create a collusion attack using SQL injection queries, our system will detect it and block it. Second, the data owner may share and revoke files to specified users or groups, and third, whenever any user is revoked, the system will issue proxy keys, which means that current keys will expire. The total strategy significantly increases system efficiency and security.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

V. CONCLUSION AND FUTURE SCOPE

We proposed a cloud computing technique and methodology for assessing security challenges related to Software as a Service attack detection and prevention in this study. We also talk about the security aspects. We look at a variety of security risks and ways for dealing with them. We also discussed other techniques to provide greater security. The proposed research focuses on online attack detection and prevention in a cloud web context. Meeting the security, privacy, and trust difficulties of cloud computing is a difficult task since it requires a mix of technical and legal solutions capable of addressing practical realities and concerns. This paper describes the unique security problems that SaaS presents, as well as how modern security testing may help guarantee that these concerns are fulfilled. Cloud computing has a number of benefits, but it also has a number of security concerns to consider. Any cloud-based service's security must be thoroughly examined in order to determine what safeguards are in place for our data. There's also the matter of accessibility. A denial of service attack or the service provider failing or going out of business might threaten this availability. The suggested system uses a power prevention method to defend against different software attacks. Initially, we created a single online application with various flaws, allowing a third-party attacker to easily launch an assault against the whole web application. You have defined some harsh monitoring foundation settings with this study that can simply eliminate any harmful connections or assaults. To test the suggested system in a multi-cloud environment with multiple attack detection and prevention mechanisms utilising machine learning techniques.

REFERENCES

1. Singh, S.; Sheng, Q.Z.; Benkhelifa, E.; Lloret, J. Guest Editorial: Energy Management, Protocols, and Security for the NextGeneration Networks and Internet of Things. IEEE Trans. Ind. Inform. 2020, 16, 3515–3520.
2. Almiani, M.; AbuGhazleh, A.; Al-Rahayfeh, A.; Atiewi, S.; Razaque, A. Deep recurrent neural network for IoT intrusion detection system. Simul. Model. Pract. Theory 2020, 101, 102031.
3. Hong, Z.; Hong, M.; Wang, N.; Ma, Y.; Zhou, X.; Wang, W. A wearable-based posture recognition system with AI-assisted approach for healthcare IoT. Futur. Gener. Comput. Syst. 2022, 127, 286–296.
4. Adil, M.; Khan, M.K. Emerging IoT Applications in Sustainable Smart Cities for COVID-19: Network Security and DataPreservation Challenges with Future Directions. Sustain. Cities Soc. 2021, 75, 103311. [PubMed]
5. Kurte, R.; Salcic, Z.; Wang, K.I.K. A Distributed Service Framework for the Internet of Things. IEEE Trans. Ind. Inform. 2020, 16,4166–4176.
6. Zeng, P.; Pan, B.; Choo, K.K.R.; Liu, H. MMDA: Multidimensional and multidirectional data aggregation for edge computingenhanced IoT. J. Syst. Archit. 2020, 106, 101713.
7. Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. Futur. Gener.Comput. Syst. 2018, 82, 761–768.
8. Farivar, F.; Haghighi, M.S.; Jolfaei, A.; Alazab, M. Artificial Intelligence for Detection, Estimation, and Compensation of MaliciousAttacks in Nonlinear Cyber-Physical Systems and Industrial IoT. IEEE Trans. Ind. Inform. 2020, 16, 2716–2725.
9. Gupta, M.; Abdelsalam, M.; Khorsandroo, S.; Mittal, S. Security and Privacy in Smart Farming: Challenges and Opportunities.
IEEE Access 2020, 8, 34564–34584.
10. Al-Haija, Q.A.; Zein-Sabatto, S. An efficient deep-learning-based detection and classification system for cyber-attacks in iotcommunication networks. Electronics 2020, 9, 2152.
11. Zhang, T.; Zhao, Y.; Jia, W.; Chen, M.Y. Collaborative algorithms that combine AI with IoT towards monitoring and controlsystem. Futur. Gener. Comput. Syst. 2021, 125, 677–686.
12. Li, B.; Feng, Y.; Xiong, Z.; Yang, W.; Liu, G. Research on AI security enhanced encryption algorithm of autonomous IoT systems.Inf. Sci. 2021, 575, 379–398.
13. Karale, A. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. Internet Things 2021, 15, 100420.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

14. Obaidat, M.A.; Obeidat, S.; Holst, J.; Hayajneh, A.A.; Brown, J. A comprehensive and systematic survey on the internet ofthings: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures.Computers 2020, 9, 44.
15. Li, J.; Kuang, X.; Lin, S.; Ma, X.; Tang, Y. Privacy preservation for machine learning training and classification based onhomomorphic encryption schemes. Inf. Sci. 2020, 526, 166–179.
16. Sarica, A.K.; Angin, P. Explainable security in SDN-based IoT networks. Sensors 2020, 20, 7326.
17. Aleem, S.; Capretz, L.F.; Ahmed, F. Security Issues in Data Warehouse. arXiv 2015, arXiv:1507.05644.
18. Wu, M.; Song, Z.; Moon, Y.B. Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods.J. Intell. Manuf. 2019, 30, 1111–1123.
19. Patil, R.; Dudeja, H.; Modi, C. Designing in-VM-assisted lightweight agent-based malware detection framework for securingvirtual machines in cloud computing. Int. J. Inf. Secur. 2020, 19, 147–162.
20. Dang, T.K.; Pham, C.D.M.; Nguyen, T.L.P. A pragmatic elliptic curve cryptography-based extension for energy-efficient device-todevice communications in smart cities. Sustain. Cities Soc. 2020, 56, 102097.
21. Moustafa, N. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets.
Sustain. Cities Soc. 2021, 72, 102994.
22. Atul, D.J.; Kamalraj, R.; Ramesh, G.; Sakthidasan Sankaran, K.; Sharma, S.; Khasim, S. A machine learning based IoT for providingan intrusion detection system for security. Microprocess. Microsyst. 2021, 82, 103741.
23. Ghosh, A.; Chakraborty, D.; Law, A. Artificial intelligence in Internet of things. CAAI Trans. Intell. Technol. 2018, 3, 208–218.
24. Bland, J.A.; Petty, M.D.; Whitaker, T.S.; Maxwell, K.P.; Cantrell, W.A. Machine Learning Cyberattack and Defense Strategies.Comput. Secur. 2020, 92, 101738.
25. Rathore, S.; Park, J.H. Semi-supervised learning based distributed attack detection framework for IoT. Appl. Soft Comput. J. 2018,72, 79–89.
26. Kasongo, S.M.; Sun, Y. A deep learning method with wrapper based feature extraction for wireless intrusion detection system.Comput. Secur. 2020, 92, 101752.
27. Chmiel, M.; Korona, M.; Kozioł, F.; Szczypiorski, K.; Rawski, M. Discussion on iot security recommendations against thestate-of-the-art solutions. Electronics 2021, 10, 1814.
28. Aldhaheri, S.; Alghazzawi, D.; Cheng, L.; Barnawi, A.; Alzahrani, B.A. Artificial Immune Systems approaches to secure theinternet of things: A systematic review of the literature and recommendations for future research. J. Netw. Comput. Appl. 2020,157, 102537.
29. Quintal, K.; Malton, A.; Walenstein, A. Biometric Signatures for Continuous Authentication. Digit. Object Identifier 2019, 23, 18–28.
30. Lu, X.; Pan, Z.; Xian, H. An integrity verification scheme of cloud storage for internet-of-things mobile terminal devices. Comput.Secur. 2020, 92, 101686.