Survey of Security Threats and Countermeasures in Cloud Computing

Annette Shajan[1] and Shanta Rangaswamy[2]
[1,2] Department of Computer Science and Engineering
[1,2] RV College of Engineering, Bangalore, India
Email: [1]annetteshajan@gmail.com and [2]shantrangaswamy@rvce.edu.in

***Abstract*—** Cloud computing is one of the most trending IT domains in recent times. It allows a user to access state-of-theart resources, technology and infrastructure with just an internet connection. In the past few decades, most global organisations have begun to migrate towards cloud computing environments because of the plethora of advantages that are provided. Cloud computing technology is now growing at a rapid rate and it has become more convenient for organisations to transfer their workload onto the cloud. It calls for less investment and promises delivery of the latest technology at a high velocity. However, security has now become a common concern for the safety of a cloud computing environment. If the cloud environment is not built securely then it can face a lot of cyber threats which take advantage of the vulnerabilities in the system. This puts the assets, resources and the data belonging to a cloud environment at risk. This paper discusses in about the top cyber threats that a cloud computing environment faces. It also covers the countermeasures and the practices that a cloud provider should follow in order to ensure that the cloud environment is robust and impenetrable.

***Keywords*—** Cloud Computing; Cyber attacks; Cyber threats; Deployment; Security.

I. INTRODUCTION

Cloud computing had risen in popularity in the last few decades because of the need for quick, accurate and portable computing. It is a universal model for easy network access to a combination of resources such as networks, servers and other storage applications. This has been a significant stepping stone in the field of computer science and IT as it has reduced the purchases, maintenance and updates which need to be made in case of managing a physical network and computer systems. Users have a multitude of benefits now as the latest technology can be delivered to them without a requirement of knowing in depth knowledge of the technology. Cloud computing has shown a phenomenal rate of growth and promises. It promises to increase the velocity of deployment of applications, improving innovation, reducing the costs all the while increasing business acumen. Virtualization has helped in maximising the power of cloud computing. It has now become an essential in most industries especially for applications such as file sharing and real-time communication and hence, half of all global enterprises are using some form of a cloud computing service. A cloud computing service is based on its network services and hence is very susceptible to a plethora of security attacks and threats. As the technology of the cloud continues to grow, there are an increasing number of ways the network could be compromised. The need to model security in cloud computing is now of utmost importance and it includes identifying the security requirements as well as the threats associated with components of the cloud architecture which form attack vectors. This also involves identifying countermeasures which can work against these known threats in order to satisfy the cloud security requirements. The paper has been structured as follows. Section II includes an overview of cloud computing- the architecture, service models and deployment models. Section III discusses the security in cloud computing- the requirements and threats faced in each service model. Section IV discusses the countermeasures for the known vulnerabilities.

II. OVERVIEW ON CLOUD COMPUTING

The National Institute of Standards and Technology (NIST) has officially defined cloud computing as ”A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [1]

A. Cloud Architecture

In the NIST model for cloud computing there exists 5 different actors in the architecture.

- Consumer: This entity could be an organisation or a person that uses services from as well as maintains a business relationship with a cloud provider.
- Provider: A provider is a supplier of a particular cloud service to interested consumers.
- Auditor: An organisation which undertakes evaluating the cloud services, assessing the

performance and security of the implementation of the cloud.

- Broker: The broker manages the use, delivery and performance of the services. They also manage the relationship between cloud providers and consumers.
- Carrier: A third party entity that is responsible for the logistics involved in bringing the service from the cloud provider to the consumer

B. Cloud Deployment Models

The deployment models are able to elicit the context of the cloud platform, services and architecture. The four deployment models for cloud service delivery are private, public, community and hybrid clouds.

1) Private Cloud: This is a deployment cloud that is purchased and utilised by a single client or organisation in an environment designed for a single entity. The network, hardware and storage that come along with it naturally are given a significant level of security. Data available in the storage can only be accessed by the client and no other party. Hence this type of environment is best suited for companies who have data which is sensitive for any other type of deployment.

2) Public Cloud: This deployment model is owned by a cloud service provider available to the public. Users can just tap into the cloud to get the latest technology without any investment in hardware or software. The customer can pay a subscription fee or just for the resources they want to use. The provider has the responsibility for the maintenance, storage, backup, etc. for the cloud environment. Public clouds tend to have a massive storage capability in order to support various businesses at the same time. However, security cannot be promised in such an environment which is open to the public.

3) Community Cloud: This type of cloud environment is similar to the public cloud, but it is intended for organisations or clients with similar concerns or the same type of requirements. It may be owned and managed by one, many or a combination of different entities or clients or organisations. The community cloud also allows several companies to work on the same project, applications or research in a single environment. Typical examples could be a group of universities who use the cloud for their research and project purposes. The management of the cloud could be off or on site or it could be managed by an external third party client as well.

4) Hybrid Cloud: A hybrid environment is a collaboration of public and private cloud models together in one environment. Parallel environments help an application move back and forth between public and private environments. These types of environments offer organisations more scalability and flexibility than any other deployment model. Nearly 58% of all global organisations have now shifted to a hybrid cloud. It is usually managed centrally by a single client.

C. Cloud Service Models

The cloud architecture consists of the front end and the back end. The front end is what the user can use to communicate with the system itself. The back end has several cloud service models namely IaaS, PaaS and SaaS. Fig 1. indicates the type of user in each model along with examples of applications.

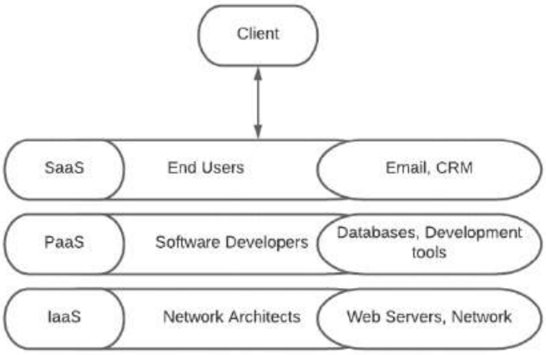

Fig. 1. Cloud Service Model

1) Software-as-a-Service (SaaS): This is the first layer of the service model. Through the data and code provided different users can access the cloud platform at the same time. This model ensures that consumers do not manage the underlying infrastructure including the application capabilities. In any SaaS application customers can code their own modifications and adjustments into the development environment as it offers several configuration options. The customers can subscribe to the service or to the resources. The entire layer is operated by a service vendor or operator. There is no requirement of any local installation of the SaaS software. This reason makes a lot of consumer's lean towards using this service model over the other service models. SaaS applications are commonly used in various editing, presentation softwares, customer relationship management tools and for tracking financial activities.

2) Platform-as-a-Service (PaaS): This second layer service model allows consumers to deploy applications onto the consumer-created cloud infrastructure. These applications could be developed with shared programming tools, processes, and APIs to speed up the development, test, and deployment of applications. There is no requirement of any software or hardware installations, hence reducing the price involved. Applications are built on top of this middleware. PaaS has tools and security built in as well as a web interface for the deployed applications. The deployed application can be integrated with other applications on the same platform and interfaced with other applications outside the platform. PaaS has software comprising a database, middleware and development tools. PaaS applications are used in business solutions, application deployment and development and testing.

3) Infrastructure-as-a-Service(IaaS): This layer is a provision mechanism allowing customers to provide the storage and computing power through networks which are critical computing resources. It is a service model that supports the provision of virtualized computing resources in the Internet. These could include storage, servers, hardware, software and various types of services available to users. IaaS can provide an abstract machine with an OS already installed. It provides for data to be stored across various geographical locations. The cloud service provider does manage the activities on the cloud, however they also provide the users the autonomy to deploy their own services onto the platform. IaaS applications are used in content delivery networks, in making highly scalable storage for storing activities and in providing a smooth backup and recovery procedure in the cloud. IaaS services where the clients can change the size of storage dynamically as needed which makes it a very scalable resource that can be adjusted as needed.

III. SECURITY IN CLOUD COMPUTING

With cloud computing becoming more prevalent and convenient to use, it has also become prone to several threats due to vulnerabilities in the system. In this section the requirements for cloud security and some popular threats faced in the cloud computing environment are discussed.

A. Cloud Security Requirements

NIST has defined the basic cloud security requirements to be similar to that of any information processing system. The requirements are stated as follows.

1) Confidentiality: Data that belongs to a user cannot be made available to any other unauthorized third party or client.

2) Integrity: The data that is stored cannot be tampered with illegally. The user must be able to trust that the data is original and is not modified without authorization.

3) Availability: The cloud data must be available and accessible to users who are authorised to use the data.

4) Privacy: The cloud user data needs to be used only for its intended purpose and for no other reason.

5) Authorization: The correct access level must be provided to the user who has subscribed for a particular set of resources, provided they have the authentication.

6) Authentication: It is the process to ensure confidence of authenticity. The identity of the user and the user’s data has to be authentic.

7) Accountability: Every action made on the cloud environment must be established as legitimate by the cloud provider to any other entity involved.

B. Cloud Security Threats

A threat could be any event with the potential to adversely impact the organisation’s mission, reputation, functions or their assets via some unauthorised access, change or deletion of data, or through denial of service. Table 1 shows top attacks performed on each type of service model and a brief description of the same. The Cloud Security Alliance (CSA) published the top eleven egregious threats in cloud computing in 2019 which are as follows. [2]

1) Data Breaches: This involves the release, viewing or stealing of protected and sensitive information by an individual who is not authorised. It could be the result of an error, inadequate security, vulnerabilities in the application or it may have been the primary goal in a targeted attack. A data breach can include information of any kind which is not intended for the public. Some examples could be personally identifiable information, personal health information, financial and trade secrets. This has been the number one security threat in the CSA ranking of 2013,2016 and 2019. Data has hence proved to be the most valuable asset of an organisation and is also the most vulnerable to misconfiguration and exploitation.

2) Misconfiguration and Inadequate Change Control: If an asset is set up incorrectly, it can lead to misconfiguration which will leave the asset vulnerable to attacks. Misconfiguration has now become a major cause for data breaches as well as unwarranted modification of resources. A common cause of misconfiguration could be the absence of effective change control. A misconfigured item can have a severe business impact depending on the nature of the misconfiguration and how quickly it is detected and mitigated. A few common examples of misconfiguration could include storage items left unsecured, unchanged default credentials and default configuration, disabling standard security controls.

3) Lack of Cloud Security Architecture and Strategy: Organisations have begun shifting their infrastructure to the public cloud. During the migration, a big challenge is that of withstanding cyber attacks with the implementation of appropriate security. Data is often left exposed to the threats as many organisations are unaware and do not understand the shared security responsibility. Functionality and speed are often given priority over the security which can leave the organisation vulnerable.

4) Insufficient Identity, Credential, Access and Key Management: These include the tools that a company uses to provide access to its resources such as files, computer systems, servers, etc. Incidents like failure to use strong passwords, inept credential protection, failure to use multifactor authentication can lead to data breaches and vulnerabilities being exposed. There can be attackers posing as authentic users who may and try to modify data, snoop on data in transit or compromise the entire system.

5) Account Hijacking: Here, a malicious actor gets an entryway into privileged or sensitive accounts. Stealing credentials, phishing attacks and exploiting the cloud system can compromise these accounts. Hijacking an account or a service can lead to a full compromise of the system- all the data and the resources are at a risk. These risks usually come from the delivery model of cloud services in which the data associated with an account reside in the cloud itself.

Table 1: Attacks in Each Service Model

Service Model	Attack	Description
SaaS	DoS	The attacker floods the service provider with bogus requests which consume the entire bandwidth and prevent a legitimate user from using the cloud service.
	SQL Injection	This is a way for an attacker to embed SQL code in order to manipulate the database in the backend. This results in information which is not meant for the public to be leaked.
	Authentication Attack	This type of attack gets the integrity and security of the data stored in the cloud in danger. An attacker may try to perform a brute force attack by trying all keys of a dictionary in order to compromise the system.
PaaS	Phishing	A popular attack in which a user is lured into clicking a link which diverts the control from the provider to the attacker site where the user might think they are providing details to a trusted source whereas in reality they are providing details to an attacker
	Man-in-the-middle attack	The channel between two parties while communicating is used by an attacker. The parties assume that they are communicating with each other, but they are, in reality, communicating with the attacker.
	Port Scanning Attack	This attack uses the vulnerabilities of the application environment itself. It gains knowledge about open ports and tries to launch attacks by exploiting these vulnerabilities.
	Metadata Spoofing	Metadata is discovered in WSDL files and it can help an attacker gain some insight about the type of data which is present in the cloud which is usually highly sensitive.
IaaS	Side Channel Attack	Parameters like the time, cache, etc which are used in cryptographic algorithms are studied in a side channel attack. This information can be useful in cryptographic software and not in the plaintext and ciphertext.
	VM rollback	In a VM rollback attack, access is gained into another user's VM by using an old snapshot of the victim's VM without their knowledge. Further the attacker can change permissions granted to the user executing rollback.
	VM escape	This type of attack involves gaining control over a guest OS or get control over the memory in order to gain access to the hypervisor

6) Insider Threat: When a person who has access and is authenticated to use the resources has the potential to misuse their access in order to negatively impact the organisation, such an entity is an insider threat. They could be current employees, former employees or business partners. Insiders do not have to penetrate through a firewall or look out for vulnerabilities because they are considered a trustworthy member of the organisation and hence has direct access to sensitive information. This type of attack leads to loss of intellectual property and sensitive data being leaked.

7) Insecure Interfaces and APIs: Providers expose a set of APIs and interfaces to the customer in order to allow them to interact with and manage the cloud services. The security of the cloud can be dependent on the security of the API. A weak security system on interfaces open to customers can leave an entire organisation vulnerable to threats that endanger the authenticity of the data. It could also have a great impact on regulations as well as financially.

8) Weak Control Plane: While migrating a service to the cloud, there is a need for data duplication and storage for which a control plane is ideal. It ensures security and integrity complementing the data plane that provides stability during runtime. A weak control plane indicates that the administrator isn't fully in control of the data and there can be certain blind spots which can result in data corruption, leakage or unavailability.

9) Metastructure and Applistructure Failures: These are critical components in any cloud service. Providers often routinely disclose security operations involved to protect their systems. The metastructure can be considered as the customer's demarcation line.

The extent of how much detail must be revealed by the provider is a critical decision. Misconfigurations can disrupt the cloud and hurt the tenants financially and in terms of operation.

10) Limited Cloud Usage Visibility: This occurs when an organisation is unable to tell whether a service running on its platform is safe or malicious. It is commonly of two major types- unsanctioned app use and sanctioned app misuse. The former occurs when users are using applications and services without permission. The latter is when authorised users leverage a sanctioned application. This can lead to unauthorised access to data and introduction of malware in the system.

11) Abuse and Nefarious Use of Cloud Services: An attacker may make use of cloud resources in order to target users. Misuse of cloud resources can include phishing attacks, self propagating malware, launching DDoS attacks, brute force attacks on stolen credentials and email spam. If an attacker has compromised the cloud infrastructure then they have more control over the provider and can cause a substantial amount of financial losses.

IV. COUNTERMEASURES FOR THREATS IN CLOUD COMPUTING

Several recommendations, countermeasures and practices have been suggested by researchers and organisations in order to keep the cloud computing environment as secure as possible, leaving space for minimal vulnerabilities. Some of these countermeasures are listed below.

A. Identity and Access Management

IAM can be explained as the ability for only the correct individuals to be granted access to the right resources at the appropriate time. Identity, authentication and authorisation of users at every level of the cloud environment is monitored and managed. Identity management involves ensuring that the user has a strong password with resetting and expiration policies which ensure that there is a cycle period for each password. Authentication involves verifying the identity of the user when they are logging in. Recommended methods are multi factor authentication with hard or soft tokens and biometrics. Authorisation is the permission given to a user in order to use a particular resource. A user must always be authenticated before they are authorised to use a resource.

B. Digital Signature and Message Digest

In order to ensure integrity, authenticity and non repudiation of data communicated between two parties over the cloud, message digest, Message Authentication Code(MAC) and digital signature are a few mechanisms that are used. Message digest encrypts the message using popular hash functions like MD5 or SHA. Digital signatures are signed with an asymmetric pair whereas a MAC uses a symmetric key. The key will authenticate the user and after that the user can establish a connection with servers and devices. In the cloud environment, a digital signature with SSO and Lightweight Direct Access Protocol provides a really strong authentication process. There are several other proposed methods which can be used as a digital signature in order to provide anonymity as well as traceability- some of which are to arrest free riders of a SaaS, providing proof of data possession, etc.

C. Intrusion detection system

These systems are able to detect any anomaly by analysing traffic activity and network traffic patterns. Intrusion detection and prevention systems are necessary at the network level and the VM instance level for any cloud environment. The network IDS will be able to detect a vulnerability caused due to authentication or authorisation intrusions, session hijacking, and back door attacks. IDS can be of a few types:

1. Network based IDS: Analysis of network packets using the signature or anomaly approach in order to detect malicious activities like DoS attacks, port scanning, etc.
2. Host Based IDS: The host file system, kernel and behaviour are monitored and analysed to detect changes, analyse the system logs against access control policies in case of an intrusion.
3. Distributed IDS: Consists of multiple IDSs over a big network and can detect any anomaly based on traffic pattern.
4. Hypervisor based IDS: This is deployed at the hypervisor level and is used to analyse and detect anomalies in the communication between VMs, the hypervisor and in the virtual network.

D. Security measures for web applications

Web services are a core technology used in most cloud environments. Hence it is extremely important for necessary countermeasures be set up in case of any vulnerabilities present in the system. Web service security uses a combination of security tokens, encryption, digital signatures, XML encryption and XML signature to provide a complete and reliable system. Web browsers which are used to access the services also need to be setup with adequate countermeasures such as setting up anti virus and anti spyware. To develop the most secure web application, software development teams need to have sufficient training in security. It is necessary to secure the Software Development Life cycle, perform regular penetration testing on web applications for a secure session management.

E. Security measures for Data Storage

Data is the most important resource for any organisation and it is essential for the storage of data to be as secure as possible subject to minimum cyber threats. Classifying data according to their sensitivity and setting up strict access controls to ensure only authorized personnel can access a certain type of data. Encrypting stored data can be a way to ensure confidentiality as well as integrity of the data. There also needs to be transparency between the provider and the client regarding backup related information like where the data will be stored, how often the data will be backed up as well as its availability. Data sanitization is an important security compliance measure which involves completely removing all traces of sensitive data before disposing or reusing an asset. These measures help to keep a robust storage system for data.

F. Network Security Measures

The CSA recommends that a cloud provider should be able to provide protection for data whilst in transit with firewalls, IDS, IPS and virtual LANs. External interfaces are protected with firewalls keeping only the required ports open. An updated intrusion detection and prevention system must be in place which analyses traffic flow over the entire virtual network. The conventional and virtual system should be connected with a hypervisor for catching abnormal packet patterns and traces. There are also proposals to validate the provider’s network security by performing penetration tests on the network, packet analysis, session management, and conducting appropriate security measures in case of any observed anomalies or deviations.

V. CONCLUSION

Cloud computing has become ubiquitous in the current day scenario with most of global enterprises shifting to a cloud based system. Hence it is important for such a system to be as robust and secure as possible minimising the organisation’s vulnerabilities to cyber attacks which can lead to loss of data, property and impose a heavy cost in damage. In this paper, functionalities of the cloud were covered, along with the most popular security threats that a cloud computing environment faces and the countermeasures to mitigate such threats in order to keep the attacks and losses to a minimum.

ACKNOWLEDGMENT

I would like to thank Prof. Ramakanth P, Head of the Department, Computer Science and Engineering, Rashtreeya Vidyalaya College of Engineering for all the guidance and support.

REFERENCES

[1] Mell, P. and Grance, T. (2018). The NIST Definition of Cloud Computing. [online] National Institute of Standards and Technology — NIST. Available at: https://www.nist.gov/ [Accessed 15 Nov. 2018].

[2] CSA, The Egregious 11 - Cloud Computing Top Threats in 2019, Tech. Rep., Cloud Security Alliance, URL

https://downloads.cloudsecurityalliance.org/assets/research/topthreats/Egregious11 Cloud-Computing Top-Threats.pdf, 2019

[3] Sharmila, K.” A Review paper on Cloud Computing Models.” international peer reviewed journal (JAC) (2020).

[4] Parthasarathy, Rajamohan, et al.” An Overview of Cloud Computing Different Services Models and Security Issues and Concerns in an Enterprises Data Storages.”,2020

[5] Odun-Ayo, M. Ananya, F. Agono and R. Goddy-Worlu,” Cloud Computing Architecture: A Critical Analysis,” 2018 18th International Conference on Computational Science and Applications (ICCSA), Melbourne, VIC, Australia, 2018, pp. 1-7,

[6] Diaby, Tinankoria, Bashari Rad, Babak. (2017). Cloud Computing: A review of the Concepts and Deployment Models. International Journal of Information Technology and Computer Science. 9. 50-58. 10.5815/ijitcs.2017.06.07.

[7] Muller, Sune, Holm, Stefan, Søndergaard, Jens. (2018). Benefits of ¨ Cloud Computing: Literature Review in a Maturity Model Perspective. Communications of the Association for Information Systems. 37. 10.17705/1CAIS.03742.

[8] Alam, Tanweer. ” Cloud Computing and its role in the Information Technology.” Tanweer Alam. (2020). Cloud Computing and its role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI) 1.2 (2020): 108-115.

[9] Patil, Sulabha & Dharaskar, Raiiv & Thakare, Vilas. (2017). Digital Forensic in Cloud: Critical Analysis of Threats and Security in IaaS, SaaS and PaaS and Role of Cloud Service Providers. 1-7. 10.1109/ICCUBEA.2017.8463984.

[10] W. Isharufe, F. Jaafar and S. Butakov,” Study of Security Issues in Platform-as-a-Service (PaaS) Cloud Model,” 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 2020, pp. 1-6, doi: 10.1109/ICECCE49384.2020.9179414.

[11] Alshammari, S. Alhaidari, A. Alharbi and M. Zohdy,” Security Threats and Challenges in Cloud Computing,” 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, USA, 2017, pp. 46-51, doi: 10.1109/CSCloud.2017.59.

[12] Sun, Panjun. (2019). Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges and Solutions. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2946185.

[13] P. J. Sun,” Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions,” in IEEE Access, vol. 7, pp. 147420-147452, 2019, doi: 10.1109/ACCESS.2019.2946185.

[14] Singh, Ashish & Chatterjee, Kakali. (2016). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications. 79. 10.1016/j.jnca.2016.11.027.

[15] Nowrin and F. Khanam,” Importance of Cloud Deployment Model and Security Issues of Software as a Service (SaaS) for Cloud Computing,” 2019 International Conference on Applied Machine Learning (ICAML), Bhubaneswar, India, 2019, pp. 183-186, doi: 10.1109/ICAML48257.2019.00042.

[16] Ramachandra, Gururaj & Iftikhar, Mohsin & Khan, Farrukh. (2017). A Comprehensive Survey on Security in Cloud Computing. Procedia Computer Science. 110. 465-472. 10.1016/j.procs.2017.06.124.

[17] Kumar, Ravi & Raj, Herbert & Perianayagam, Jelciana. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. Procedia Computer Science. 125. 691-697. 10.1016/j.procs.2017.12.089.

[18] Alhenaki, Lubna & Alwatban, Alaa & Alamri, Bashaer & Alarifi, Noof. (2019). A Survey on the Security of Cloud Computing. 1-7. 10.1109/CAIS.2019.8769497.

[19] S. Basu et al.,” Cloud computing security challenges & solutionsA survey,” 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2018, pp. 347-356, doi: 10.1109/CCWC.2018.8301700.

[20] Cook, Allan & Robinson, Michael & Ferrag, Mohamed Amine & Maglaras, Leandros & He, Ying & Jones, Kevin & Janicke, Helge. (2017). Internet of Cloud: Security and Privacy issues.

[21] Kumar, Rakesh & Goyal, Rinkaj. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review. 10.1016/j.cosrev.2019.05.002