**A Cloud Computing Security Framework Derived fromWeighing Vulnerable Areasfrom User’sPerspective**

**A**

**SYNOPSIS**

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **Sr.No** | **Name** | **Page No.** |
| 1. | Introduction | 1 |
| 2. | Statement of Problem | 2 |
| 3. | Literature Review | 3 |
| 4. | Research Gap | 11 |
| 4. | Need for the Research | 12 |
| 5. | Objectives of the Research | 12 |
| 7. | Scope of the Research | 13 |
| 8. | Research Methodology | 14 |
| 9. | References | 15 |

1. **Introduction**

Cloud Computing has retained its position as the most sought after technology in IT since 2007. Cloud Computing is a system of computing on internet. The most prominent features of Cloud Computing are: cost saving, high speed computation, sharing on demand, elasticity, reliability, scalability, pay as you go. Cloud Computing enables users to access multiple online resources to process, manage and store data instead of using single separated personal computer. Its aim is to broadcast computing services to end user. These resources are dynamic and scalable which can be accessed through the internet from anywhere at any time without worrying about its technical and physical management or maintenance issues. Google is the chief example of Cloud Computing [[1](#Rao15)].One of the broadly used definitions of Cloud Computing by NIST is as: “Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management service provider interaction or effort”[[2](#Tar16)].

Although Cloud-based services are now becoming the part of our daily, security issues are the main barriers and hurdles toward the rapid growth of Cloud Computing. As Cloud Computing allow group of users to access online shared data, so there is a possibility of high risk of security[[1](#Rao15)] .Cloud Computing is prone to numerous threats and vulnerabilities. These threats are a combination of network security, data security, application security, server security, web security, authentication & authorization security and virtualization security threats. Cyber-attack is one of the prominent issues in the network security and data security threats[[3](#Nih17)].Cloud Computing has received more attention over the past few years to understand its security issues. Security threats can occur not only from outside but from within the organization also. According to the Cyber Security Watch Survey conducted on 607 businesses; government executives; professionals and consultants, 21% of cyber-attacks were caused by insiders [[2](#Tar16)]. The most common insider attacks were unauthorized, unintentional disclosure of sensitive data, virus, worms and stealing of intellectual property. Four thousand ransomware attacks per day were found by FBI in the year 2016. Moreover, victims and law enforcement officers are suffered by 26 crypto-ransomware attacks for last four years[[4](#Len19)]. Hence hackers are getting an unauthorized access of consumer’s data on the cloud. They are stealing confidential information for illegal activities, via various techniques[[5](#TeS131)]. In magazine, named ‘PC quest’ published under the issue 8, Vol.32 in August 2019, Executive Editor Sunil Raj Guru highlights cyber security as major concern in 2019.

Moreover, many breaches also have been seen at different places in the same year. Baltimore, Atlanta and few other towns have been affected with these threats. Florida municipalities in US also have paid $ 1 million to attacker after ransomware cyber-attack.

As India is increasingly growing digital, it is also facing the fear of cloud breaches by unauthentic users. According to Alvin Rodriguez, Senior Director of security strategist, organizations are facing security issues from insider as well as outsider threats now days. Another most common type of cyber-attack is Social Engineering attack which is carried out through email, web sites, downloads, spear phishing and identity compromise. The insider threats occur unintentionally, and users remain unaware about them[[6](#OFa19)]. Moreover, existing studies elaborate many threats that need to be resolved urgently in the Cloud Computing. It is an accepted that major improvement is required in security policy on cloud platform because of its hosting platform. Hence, significant advancement in security mechanism is required to achieve higher level of security [[7](#Ram17)]. Most of the researches studies, analyze threats only to cope with security issues, whereas vulnerabilities have a major role to play towards solving security challenges on Cloud Computing platform.

In our study we will attempt to hedge the vulnerabilities from the perspective of users on cloud platform.

1. **Problem Statement**

In the scenario of increasing dependability of cloud computing, the increase in threats and vulnerabilities poses as a credible threat to cloud incorporation. Every consumer who is planning to take advantage of cloud technology, needs to be aware about its vulnerabilities and threats that have potential to cause serious damage, to cope with security challenges. The vulnerabilities of Cloud platform lead to the hackers to make damage and violation.

The important challenge in the Cloud Computing is that cloud network should provide all necessary security measures to protect the data from the hackers. A lot of the research on security mechanisms is being carried out, such as addition of extra and complicated firewalls, however, the threats still prevail. Many security mechanisms have been proposed by different researchers and scholars to neutralize the threats. Moreover, hedging the vulnerabilities also has a major role to play towards solving security issues in Cloud Computing.

Since, the dependability of cloud computing is increasing in an exponential manner, more and more threats towards cloud computing platform are being developed. As told earlier, there have been many researches in order to understand the different threats which characterize the cloud computing platform. However, there is almost no research to identify the various vulnerable areas for the cloud computing platform and developed strategies to identify the possible threats and safeguard oneself from them.

The current research will not only identify the different vulnerable areas based on the cloud computing usage platform, but also suggest a framework for highlighting the vulnerabilities and find out different remedies to secure oneself from these potentials threats.

In addition, the research would also understand the impact of incorporation of different strategies for protection against cloud threats on the working of applications for the cloud user. These different strategies will be critically analyzed based on the level of sensitivity of the data, or tradeoff of the security technique – performance will be brought out.

Hence, this research will be most beneficial in today’s times where it is increasingly important for the user to become aware about the vulnerable areas in cloud computing platform and equip himself with strategies to resist cloud threats without compromising on performance.

1. **Literature Review**

The security of cloud services is dependent upon the security of APIs. It is standard software based interface through which user manage the services[[8](#Moh15)]. Cloud service providers and third parties use application programming interfaces to offer different services to customers [[9](#Man13)]. Poor interface of APIs pave the path for hacker to access secret key that can lead damage of integrity,confidentiality and availability[[10](#Muh15)].Moreover, robustness in access and identity management is required in API, which otherwise facilitates the attackers to access secret information on cloud [[11](#Ibt18)]. Data breach is another threat having severe risk and it is ranked as number one among the threats in Cloud Computing. It is another incident in which sensitive, private, or confidential data related to a person or organization is being accessed, copied, or transmitted by an unauthorized party. In 2017, over 1.4 billion records were lost due to data breaches. [[12](#Sur18)]. Many prominent sites including Facebook, Gmail, Youtube, LinkedIn has been mistreated for data breach. Mostly data breach occurs because of malware; theft or stolen computers; insider attempt and attacks by an unauthorized user [27].Moreover, networking, authentication protocols, human error, and application infrastructure vulnerabilities provide attackers with single point of attack[[8](#Moh15)].Many of the authentication protocols are also error prone and they need to be verified by testing tools[22]. Moreover, an account theft can be performed by different ways, such as social engineering and weak credentials. If an attacker gains access to a user’s credential, he can perform malicious activities like redirect any transaction and manipulation of data[[13](#Muh18)].Account or service hijacking is social engineering attack that occurs during the sharing of account credentials between users and services and affects its privileges access through Malware injection attack. It also involves phishing, fraud and software vulnerabilities [[14](#Iss141)].According to latest survey, phishing is second most critical cyber security issue after data breaches. Phishing term describes a malicious individual or group of individuals who trick users by sending e-mails or creating web pages[15]. Malicious insider is an dedicated insider that uncovers different ways to attack over the cloud[[7](#Ram17)]. They get hands on an unusual quantity of information to produce various kinds of damage to the customers’ assets [[11](#Ibt18)]. Additionally, they collect an individual's online bank, credit card in order to steal credentials and gain an unauthorized access [[14](#Iss141)][[9](#Man13)].Consequently, the userswouldhavetocompromisewith cloud servicesbecause of its credentials theft[[15](#Men)]. Subsequently, password authentication is evaluated as the weakest among all mentioned authentication method.There are two types of password guessing attacks: Brute Force attacks, through which attacker guess the password by getting each possible combination; Dictionary attacks, detect the password from dictionary of common words [22].On cloud platform, malware program is used to steal password and transmit credential information to hacker. It is further classified as follows: virus, browser hijacking, spyware software [27].

Ransomware is another type of malware that spread by attacker on consumer’s system for the purpose of money. It is like a worm that spread across the user system and lock the system and files within the system. It confines users from accessing their system, either by locking the system’s screen or by encrypting users' files, unless ransom is paid [[16](#Nad17)]. Ransom ware can come from multiple sources like email, video, PDF file or a website link, a connected device, or even by a password hacking. Ransomware is basically a malware which stores itself in the cyber physical system and it must cross through the firewall of the system to penetrate into various files. Therefore, the firewall becomes a vulnerable area for the ransomware threat. In addition, this threat may propagate from various sources available on the internet.

Next, Denial of Service (DoS) and Distributed Denial of Service (DDoS) are most well-known attacks that take place when attacker overflows network’s traffic by flooding the fake request on network. This attack makes the services unapproachable for legitimate users. DDoS is more dangerous to cloud computing in comparison to other internet based[[17](#Mrh18)].These false requests consume processor power, memory, disk space, and network bandwidth and make the system slowdown [[8](#Moh15)].So flooding is the most common way in which the hackers deteriorate the victim’s system by overwhelming bogus requests [[13](#Muh18)].Consequently, this attack makes legitimate users unable to access the services of cloud. There are two types of DOS First directDoS and second indirect DoS [[3](#Nih17)].

The term due diligence refers to individuals or customers having the complete information for assessments of risks associate with its services. Insufficient Due -diligence leads unknown operational risk in cloud [[10](#Muh15)][[8](#Moh15)].Data on the cloud can be evidently lost because of malicious attack, accidental removal by the cloud service vendor and physical disaster. All of these threats seem to cause the permanent loss of user’s data [[11](#Ibt18)].Moreover, Data leakage takes place when it gets into the wrong hands while it is being transferred, stored, and audited or processed [[13](#Muh18)]. User lost his control over the data backup procedure, file systems, redundancy, security policies, and other relevant configurations when it is being transferred on the Cloud[[9](#Man13)]. Unreliable media or communication channel, natural disasters, human errors, physical infrastructure, weak passwords, internet basic security are other many cause of data loss or leakage and alteration of records [[12](#Sur18)]. Moreover, an unreliable media or unsecure communication channel are other vital source of Meta data spoofing attacks[[9](#Man13)]. Furthermore hardware or system malfunctions such as natural disasters (floods, earthquakes; simple human errors (accidentally deletes files), hard drive failure, and power failure)also lead to the data loss. Data leakages have a severe impact on organization due to shared resources [[17](#Mrh18)]. Legal and compliance aspects point out the responsibilities of user or client that must be operate in accordance with established laws, regulations, standards, and specifications. Security, followed by issues regarding compliance, privacy and legal matters is the most significant barrier [[13](#Muh18)]Vendor lock-in is another foremost barrier in acceptance of Cloud Computing services [[15](#Men)][[18](#Jus16)]. Vendor Lock attack occurs when consumer becomes dependent on a service provider and cannot migrate to another service provider [11]. Vendor lock attack occurs due to the lack of standardization, heterogeneity of semantics and application program interfaces, which further leads portability and interoperability challenges[32]. In this way portability, interoperability and cloud federation are main three lock-in effects that cause vendor lock-in[[15](#Men)]. Portability is the ability that make cloud user able to move his applications, data, and tools from one cloud vendor to another in a company, and interoperability allows different clouds to communicate with each other. The problem of interoperability occurs because of different APIs by service providers [8].Therefore vendor lock-in can be avoided by achieving interoperability and portability among different cloud provider[[18](#Jus16)].Cryptojacking is new emerging cyber attack which mainly hires the CPU power of other person’s computer to extract cryptocurrency. This is done either by getting the victim to click on a malicious link in an email,orby injecting malicious JavaScript code into websites for loading Cryptomining code on the computer and for mining Cryptocurrency respectively.In-browser, a Cryptojacking becomes a major problem as it involves hijacking of CPU power of a website’s visitor to perform its own CPU-intensive task[19].

According to Wall & Connolly [4], Mostly users are unaware about the sites having cryptojacking. In order to accomplish a cryptojacking attack successfully, the attacker infiltrate into the cyber physical system and hire processing power without the consent of legitimate user. However, on websites this type of attack executed through storing cookies on computer. Consequently malware slow the processes running on user’s system, but users are completely unaware about cryptojaking attack. The type of security certificate that is installed by the website is very critical for prevention of such attack[[4](#Len19)].

Despite mentioned threats there are many forms of attacks that are responsible for poor quality of computing. Dhote et al.[[19](#Lon17)] described all enterprises threats into two forms: Intentional and inadvertent. Intentional threats are external threats that occur due to malware, virus, Trojan, hacking and social engineering. Inadvertent threats are insider threats that take place because of accidental publishing, configuration error, improper encryption, missing computer, privilege abuse. Hence Al-Saleh & Hamdan [33], groupedsecurity issues into six groups: network security: cover issues related to configuration and communications; storage security: cover up data confidentiality, integrity and availability; governance: includes issues related to procedures, policies and security method of deployed: services hypervisor: an identity and management security; legal and compliance: issue related to laws, standards, regulations, and specifications.

Kaur& Kinger[[20](#Kin14)]described encryption as a prominent countermeasures against data breach. Encrypted data prevent attacker to deduce the crucial information from data itself. There are two types of encryption: Symmetric and Asymmetric. Symmetric includes methods such as 3DS, Blowfish and AES whereas Asymmetric key encryption consists: RSA, Diffie-Hellman and Elliptic Curve. These are basic primitives for cryptographic. Advanced cryptographic techniques are classified as follows: Public Key Method and Format Preserving Encryption. Public Key Method further comprises Functional Encryption (FE), Identity Based Encryption (IBE), Attribute Based Encryption (ABE), Homomorphic Encryption (HE), Verifiable Computation (VC) and Secure Multiparty Computation.

According toKumar & Deepti[[21](#San17)] strong authentication and authorization mechanisms play vital role toward security on the cloud platform. Authentication ensures a user identity and authorization process verified the access rights of the user having request to particular resource. To make it effective some mechanism such as password, smart card, fingerprint, digital certificate are in use to verify the requesting party. But poor authentication leads many threats such as loss of privacy and integrity, identity spoofing risk. Password authentication is evaluated as the weakest among all mentioned authentication method.Currently JSKY tool is in use for both Gmail and Yahoo server to test the authentication service.

Rahman et al.[[22](#MAD18)] illustrates OffPAD towardsolving man-in-the-middle and phishing attacks. Offline Personal Authentication Device (OffPAD) is new version of Personal Authentication Device (PAD)having significant role to manage and authenticate a user. It provides many tools to manage authentication. HTTP Digest Access Authentication system having Cryptographic Hash function is used to produce message digest,but it does not provide complete security againstman-in-middle and replay attacks.

Rashmi& Deshmukha[[23](#Ras15)] elaborate Intrusion detection System to assists cloud consumers against explosion of DDoS. An IDS includes method: Anomaly detection and Misuse detection[20].Anomaly detectionmethod compares the current abnormal behavior of system with previously recorded normal behavior of the system, in order to detect attack on cloud platform. Moreover, IDS mechanism detects attacks by discovering false positive in behavior of the system. It further includes NOMAD;D-WARD;MULTOPS; PacketSampling; and Filtering techniques with Congestion.MD method detected attack by keeping database of commonly used signature pattern. After getting matching pattern, the system having message detection method will indicate toward DDOS[24]. Hybrid Intrusion Detection technique [20] beats the loopholes of Anomaly detection and Misuse detection methods.Moreover, it can be efficiently implemented on any cloud platform such as private, public and hybrid [20].

Theng & Kene[[24](#Sne15)] state that although, traditional firewall method is in use to secure the system against outsider attack but it is not able to cope with insider as well as complicated outsider denial of service attacks. To deal with attack under the category of : insider, outsider, known and unknown attacks, author explained four types of Intrusion Detection System named Host based, Network, Distributed, and Hypervisor has been introduced. NIDS detects the DOS and Port Scanning attacks on network traffic. HIDS gathers information from host and detect unauthorized events to maintain integrity. HIDS locates the anomalous action of user by getting conversationdetail within hypervisor based network. DIDS(Distributed IDS) is combination off all mentioned IDSs. Although many Intrusion Detection Systems have been proposed, but all are fail to detect unknown threats. Although these techniques are useful in detectingintrusions on cloud platform but all are unable to provide complete security. Another Cloud Intrusion Detection Model, by Bhatti et al.[[25](#Upm13)] comprises Anomaly based detection system along with Entropy mechanism to detect attacks.Entropy is used to assess the randomness of data over cloud.A fixed threshold value of Entropy detects DDoS attacks. Entropy-based Anomaly Detection System helps the user to detect and block the attack before reaching it to the victim’s system [26].

According toRanjithprabhu et al.[[26](#Nan14)]data breach is on the top among all threats. In his paper they focused on three aspects: data governance, secured architecture and securedinformation to control data breach activities. Data governance comprises three actions such as risk assessment, secure disposal and retention policy to monitor, manage, maintain and protect data on cloud. Information Security measure encompass encryption and encryption key management. Both of them have significant role to protect user’s data on cloud. Moreover, other parameters that effects cloud security architecture are login credentials, authentication and data integrity. All strategies play its role in designing trusted security architecture.

Yesilyurt & Yalman[[27](#Mur16)]summarize data security into four terms: data integrity, data confidentiality, data audit and accessibility.To achieve mentioned features, they preferredData hiding techniques to prevent data from being read by malicious users. Techniques are classified further as: steganography, watermarking and cryptology. These techniques are appreciated for its robustness and access security.

In cloud, cryptojaking is emerging as major threat in these days on network and device. Cryptojacking is an unethical access of computer power without the consent of users. The websites having cryptojacking script will degrade the performance of system that is being used for accessing effected website. Shastri et al. [28] highlights browser extension feature to provides graphical interface to verify such type of websites [[28](#Shu191)].The system with browser extension facilitates a user to match the URL of Script with the list of URLs stored in the database. The extension will make user aware about effected websites. Browser extension provides blocking feature also, which enables a user to block malicious script and access the website without worrying about CPU power theft. Furthermore, Wressneggeret al. in [[29](#Mar18)] recommended two more strategies such as: Addblocker and antivirus against the cryptojaking threats. Add blocker is one of the efficient and cost effective solutions to protect the user’s system from cryptocurrency mining. Blacklists and browser extensions protection method are efficient only for known mining sites but unable to provide sufficient protection against modified variants mining code.

According to Prajapati & Surati[[30](#Son17)] ransomware attack is being effective in multiple forms since 1983.But basically it has main three families named: Ransomlock, PCyber and Cryzip to effect the system by blocking or moving data from the victim’s system. Many cyber security schemes have been proposed against ransomware attack. In order to implement security on system against ransomware, all techniques pass through four phases named: predicate, prevent, response and detect. Anticipation techniques and closer attention on access rights are other basic recommendation against Ransom attacks. Detection and Prevention techniques are classified further as follows: Honeypot, Heldroid, Cryptolock and Sandbox. Hence, there are many ways through which Ransomware can affects system, but these are broadly classified into main three types such as Scareware, Lock-Screen and Encryption. According to Baris Celiktas[[31](#Bar18)] Anomaly based detection system is an efficient method in data analysis, which further helps in detecting the behavior of Ransomware. Moreover, hybrid approach which is combination of both Signature based and Anomaly based approach is more efficient as it is successful in detecting and preventing Ransomware attack with minimum file loss and false-positive rate from threats. The hybrid approach grantsearly warning to the consumer and prevents the Ransomware from running it on consumer system. It has two phases “training/learning” and “monitoring/detecting”. This method is preferred more because of its capability in minimizing false positive, file loss. Moreover, it is also flexible and inexpensive.

Opara-Martinset al. [18] mitigate and overcome the risks of vendor lock-in.Various standards and methodologies such Open Virtualization Format (OVF)) and Amazon S3 API has been adapted for application migration and data migration respectively. Portability and interoperability are top most themes in vendor Lock-in.Vendor Lock-In occurs due to heterogeneity in semantics and cloud Application Program Interfaces (APIs).it creates technical incompatibility which in turn leads to interoperability and portability challenges. Open Virtualization Format (OVF)) and data migration standards address application migration by mitigating lock-in concerns.

Liuet al.[[19](#Lon17)]describedDLPD systems to indentify, monitor and avert intentional disclosure of susceptible information in companies. It includes content-based and context-based analysis. Content based analysis inspects the content at different level such as transit, in use and at rest to protect the data. Context-based approach performs contextual analysis of the data. This approach keeps database of commonly used data access patterns to detect the unauthorized request. It produces an alert alarm when any matching access pattern found.

Sahanaet al.[32] Virtual Private Network and Firewall techniques ensure security on the cloud platform.VPN mechanisms allow a user to create a tunnel, through which the user can access cloud services securely on insecure network and protect information from being corrupted over cloud network. Therefore, firewalls define policies having many filtering rules for transaction on the network. If information go through filtering rules only then it will be allowed to travel on the cloud network, or blocked otherwise.VPS with IP is an extended way to implement the security. Firewall has vital role to play in security implementation as it filters each incoming packet and lies between internal network and outside world. A combination of both firewall and VPN provides better specific access to server.

Al-Saleh & Hamdan[33] declared that Antivirus (AV) is an essentials well as last line defense mechanism for to the end-users from all security controls such intrusion detection systems, intrusion prevention systems, Firewalls, encryption techniques. AV sheltered data by detecting the virus against its database having signatures of virus. Antivirus plays significant role in maintaining security but sometimes it is avoided by end user because of its bad effect it I on performance of network platform. Agbenyegah &Asante[34] reveal that security policy such as firewall adversely affects the performance of network. The study also state that network security and network performance are inversely proportional to each other. Most of the security mechanism has been imposed on network without knowing its bit possessing and computation need, as each of them leave its effects on network performance. Hence,Chandrashekharet al.[32] evaluates trade-off between security and performance. According Al-Saleh & Hamdan[33] delay in system is slightly more without VPN as comparative with VPN in Cloud Computing,whereas integration of firewall and VPN decrease the throughput of the system.

It feeds each coming out the at theThe above mentioned literature elaborates various threats and countermeasures against security challenges on Cloud platform. The study not only make user aware about various threats and its possible threats but also pave the path to devise an appropriate framework to manage the security issues.

1. **Research Gap**

While the domain of Cloud computing security is on high priority of researchers since the penetration of cloud services in the day to day lives of users is increasing exponentially. However, it is interesting to note that despite the increasing focus of researchers on the cloud computing security, there is an absence of research which understands the vulnerable areas which are exploited by attackers to induce different malwares / viruses in the system. Till the time the vulnerable areas are highlighted and caution activities are highlighted, the trend of new and smarter viruses will continue. The present research, therefore, aims to bridge this gap in the existing research regarding the vulnerable areas for cloud security. This research would not only study and understand the various vulnerable areas, but would also go on to highlight the different counter measures to prevent such attacks.

Hence, the current research will be catering to the most important issue in Cloud Computing security by understanding the various vulnerabilities of cloud computing from the user’s perspective.

1. **Need for the Research**

Cloud Computing is becoming popular in each sphere of life. Several security threats and vulnerabilities challenges have a vital role to play towards resisting different organizations to adapt to Cloud Computing.

A “Threat” is any potential danger toward information or systems that exploit vulnerable area is an attempt to cause damage or destruct the system. Most of the previous studies focus on threats only whereas vulnerabilities are vital to ensure effective and large-scale implementation of Cloud Computing. The vulnerable areas on cloud network are being exploited by attacker for malicious purpose. So to cope with threats, there is a need to hedge the vulnerabilities on cloud platform to avoid the security issues. Moreover, security is more uncertain to the consumer. Users, access Cloud services mostly through main three spheres named CPS, Web Sites/Softwareand Social Networking Sites. However, attackers try every possible way to break into systems and make violations. Vulnerabilities surrounded by these areas are more doubtful to the users.

In our study we will deduce threats through these vulnerabilities and then we will devise a framework on these vulnerabilities to tackle the malicious attempts. This framework will be helpful in circumventing the current vulnerabilities in the Cloud Computing.

Existing studies also show that security and performance efficiency is inversely proportional to each other. Although it is not possible in all situations, there is trade-off between the performance and security level. As Antivirus plays significant role in maintaining security but sometimes it is avoided by end user because of its bad effect it I on performance of network platform. Thus evaluation of trade-off between security and performance pave the path to find an appropriate solution framework as per user or organization’s variant requirement and preferences.

1. **Objectives of the Research**

The current research aims to comprehend the various vulnerabilities in the cloud computing platform. The following are the specific objectives for the research.

1.      To study various vulnerabilities that causes threats on Cloud platform.

2.     To devise a framework for circumventing studied threats on Cloud platform from user’s perspective.

 3. To design a suspicious behavior detection system for potential vulnerability in the cloud system.

4.      To bring out the best security - performance trade-off for hedging the vulnerabilities in cloud platform.

1. **Scope of the Research**

The current research will appraise threats from the perspective of vulnerabilities. Cloud consumers access Cloud Computing services mainly through three interfaces: Cyber Physical Systems, Softwares (Web Softwares) and social networking sites. The research study will elaborate not only the threats from the perspective of users but also classify them among three domains. In order to ensure the security, the research attempts to address every possible vulnerability attribute on the Cloud Computing platform from the perspective of users. Thereafter, the research lists various precautions and their corresponding strategy, which can be adapted by the users in order to minimize Cloud Computing operations risk.

The aim of our research is to uncover the following through the process of empirical investigation:

* The research will clearly define the concept of Cloud Computing platform and its security challenges.
* Subsequently, the research will deduce various vulnerability attribute on Cloud Computing platform from the perspective of users.
* The research will highlight each possible strategy against threats on Cloud Computing platform.
* The present research will propose new strategies for users through which they can ensure effective implementation of Cloud Computing.
* The current research will also evaluate trade-off between security and performance of security strategies on Cloud Computing platform
* The present research will also design behavior detection system to minimize the risks towards Cloud Computing platform.

1. **Research Methodology**

The present research will follow a systematic approach to address the security and privacy challenges in the Cloud Computing. Firstly, we will perform critical review of threats from the perspective of vulnerabilities. Having a list of threat and vulnerabilities, we will cluster them into three critical segments named CPS, Web Services and Social Networking Sites.

Secondly, we will devise a framework for circumventing the threats on cloud system by taking into account various vulnerabilities. To accomplish this task, we will figure out all countermeasures against each threat based on existing study. Once new approach comes into existence then we will find out the trade-off between security and performance.

And finally, based on mentioned vulnerabilities, threats and their corresponding countermeasures, we we will design behavior detection system that will make user aware about potential vulnerabilities that are common on the cloud system.

In order to do justice to the research findings, we plan to use the below stated secondary data.

Secondary data

* Peer-reviewed journals on Cloud Computing
* Previous researches
* Previous Articles and Journals
* Reports and Magazine

1. **References**

|  |  |
| --- | --- |
| [1] | R.V. Rao &K. Selvamani, "Data Security Challenges and its Solutions in Cloud Computing", in *International Conference on Intelligent Computing, Communication & Convergence*, pp. 204-209, 2015. |
| [2] | D. Manivannan ,T. Islam & S. Zeadally, "A Classification and Characterization of Security Threats in Cloud Computing", *International Journal of Next-Generation Computing*, vol. 7, pp. 1-20, 2016. |
| [3] | A. Jangra &N. Singh, "Challenges and Prosperity Research in Cloud Computing", *International Journal of Computer Trends and Technology*, vol. 49, pp. 200-205, July,2017. |
| [4] | D.S.Wall & L.Y. Connolly, "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures", *Computers and Security*, vol. 87, pp. 1-18, November, 2019. |
| [5] | T.S. Chou, "Security Threats On Cloud Computing Vulnerabilities", *International Journal of Computer Science & Information Technology*, vol. 5, pp. 79-88, June, 2013. |
| [6] | R. O’Farre, "The many Dimension of Hyper-Convergence", *Magazine PC Quest*, vol. 32, no. 8, August, 2019. |
| [7] | G. Ramachandra, M. Iftikhar, & F. A. Khan, "A Comprehensive Survey on Security in Cloud Computing", *The 3rd International Workshop on Cyber Security and Digital Investigation*, vol. 110, pp. 465–472, 2017. |
| [8] | M. Farik &S. Pandey, "Cloud Computing Security: Latest Issues & Countermeasures",*International Journal Of Scientific & Technology Research Volume*, vol. 4, no. 11, pp. 27-30, 2015. |
| [9] | C A Dhote, D. H. Sharma& M. M. Potey, "Cloud Computing – Understanding Risk, Threats, Vulnerability and Controls: A Survey", *International Journal of Computer Applications*, vol. 67, pp. 9-14, April 2013. |
| [10] | S.Y. Zhu& M. Kazim, "A survey on top security threats in Cloud Computing" , *International Journal of Advanced Computer Science and Applications*, vol. 6, pp. 109-113, 2015. |
| [11] | I.M’rhaoaurh, C.Okar, A.Namir&N.Chafiq, "Challenges of cloud computing use: A systematic literature Review", in *MATEC Web conferences* :*International Workshop on Transportation and Supply Chain Engineering*, vol**.**200, September, 2018. |
| [12] | P.S Suryateja, "Cloud Service Models Threats and Vulnerabilities: A Review",*International Journal on Future Revolution in Computer Science & Communication Engineering*, vol. 4, no. 4, pp. 563-567, 2018. |
| [13] | A. Khormali,A. Mohaisen &M. Saad," End-to-End Analysis of In-Browser Cryptojacking",*Cornell University, Computer Science, Cryptography and Security, arXiv:1809.02152v1*,September,2018. |
| [14] | A. Khreishah, M.A. Issa& M. Khalil, "Cloud Computing Security: A Survey",*Computers 10.3390/computers 3010001*, pp. 1-35, Mar. 2014. |
| [15] | M. Ashraf &F. Kamel," Vendor Lock-in in the transition to a Cloud Computing platform",*Degree Project, In Communication Systems (Ik223x), Second Level Stockholm, Sweden*,pp.1-42,2015. |
| [16] | M. Farik & N. Shah, "Ransomware-Threats, Vulnerabilities And Recommendations", *International Journal Of Scientific & Technology Research*, vol. 6, no. 06, pp. 1-18, 2017. |
| [17] | A. Backe&H. Linden,*"*Cloud Computing Security: A Systematic Literature Review" ,*Uppsala University Department of informatics and media,pp.1-43,May,2015.* |
| [18] | J. O. Martins,R. Sahandi & F. Tian, "Critical analysis of vendor lock-in and its impact on Cloud Computing migration: a business perspective", *Journal of Cloud Computing: Advances, Systems and Applications*, pp. 1-18, 2016. |
| [19] | L. Cheng, F. Liu & D. Yao "Enterprise data breach: causes, challenges, prevention, and future directions", *Wires Data Mining and Knowledge discovery.*, vol. 7, pp. 1-14, September/October 2017. |
| [20] | R. Kaur&S. Kinger, "Analysis of Security Algorithms in Cloud Computing",*International Journal of Application or Innovation in Engineering & Management*, vol. 3, no. 3,pp.171-176, March,2014. |
| [21] | S.K. Mandal &A R Deepti, "An Efficient Identity Based Authentication Protocol By Using Password",*International Journal of Network Security & Its Applications*, vol. 9, pp. 53-65, 2017. |
| [22] | M. Alhaidary, S.M.M. Rahman,M. Zakariah,M. S. Hossain,A.Alamri,M. S. M. Haque & B. B. Gupta, "Vulnerability Analysis for the Authentication Protocols in Trusted Computing Platforms and Proposed Enhancement of the OffPAD Protocol", *Article in IEEE Access · January 2018*, vol. 6, pp. 6071-6081, 2018. |
| [23] | K.K. Rashmi& V. Deshmukha, "Understanding DDoS attack &its effect in Cloud environment", *Procedia Computer Science*, vol. 49, pp. 202-210, 2015. |
| [24] | D.P. Theng &S. G. Kene, "A Review on Intrusion Detection Techniques for Cloud Computing and Security Challenges” ,*IEEE Sponsored 2nd International Conference On Electronics And Communication Systems*, pp. 227-232, Feb. 2015. |
| [25] | G. Bhatti , S. Mehmi &U.Goyal, "A Dual Mechanism for defeating DDoS Attacks in Cloud Computing Model",*International Journal of Application or Innovation in Engineering & Management ,* vol. 2, no. 3, March 2013. |
| [26] | K.Ranjithprabhu,M. Raja& C.Nandhakumar, "Counter Measures For Data Breach In Cloud Computing", *International Journal Of Research In Computer Applications And Robotics*, vol. 2, no. 11, pp. 124-129, November 2014. |
| [27] | M. Yesilyurt &Y. Yalman, "New approach for ensuring cloud computing security: using data hiding methods",*Article in Sadhana Indian Academy of Sciences* , vol. 41, no. 11, pp. 1289–1298, November 2016. |
| [28] | S.Shastri, S.Iyer, N. Patil , S. Patil & Prof. Vijay, "Browser Extension for Cryptojacking Malware Detection and Blocking",*International Research Journal of Engineering and Technology*, vol. 06, no. 04, pp. 1691-1693, 2019. |
| [29] | C. Wressnegger, M. Johns, K. Rieck & M. Musch, "Web Based Cryptojaking in the Wild",*Report in Institute for Application Security, Germany*,pp.1-33, 2018. |
| [30] | G.I. Prajapati& S.B. Surati, "A Review on Ransomware Detection & Prevention",*International Journal of Research and Scientific Innovation* , vol. 4, no. 9, pp. 86-91, September, 2017. |
| [31] | B. Celiktas," Analysis, "The Ransomware Detection And Prevention Tool Design By Using Signature And Anomaly Based Detection Methods",*M.Sc*.*Thesis*, *Istanbul Technical University Informatics Institute, pp.1-74,* May,2018. |
|  |  |
| [32] | A M. Chandrashekhar,K. Sahana & K.Yashaswini, "Securing Cloud Environment using Firewall and VPN",*International Journal of Advanced Research in Computer Science and Software Engineering Research.*, vol. 6, no. 1, pp. 151-156, January, 2016. |
| [33] | I. Mohammed, A. Saleh & H.M. Hamdan, "On Studying the Antivirus Behavior on Kernel Activities", in *International Conference on Frontiers of Information Technology (ICFIT 2018), At Paris/France* pp. 1-6, April, 2018. |
| [34] | F. K. Agbenyegah & M. Asante "Impact Of Firewall On Network Performance ", *International Journal Of Scientific & Technology Research*, vol. 06, no. 03, pp. 32-38, March,2017. |
|  |  |
|  |  |
|  |  |
|  |  |

x

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

x