Enhancing Cloud Security By Using Secure Apis In Business Enterprises In The USA

Glory

DOI: 10.29322/IJSRP.14.01.2024.p14531 https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14531

Paper Received Date: 20th December 2023 Paper Acceptance Date: 20th January 2024 Paper Publication Date: 30th January 2024

Abstract- Cloud security is a discipline dedicated to securing cloud computing systems by ensuring that data and privacy of individuals and organizations are safe across online-based infrastructure, applications, and platforms. Whether it is an individual, enterprise or small to medium businesses, any user who uses cloud services should ensure the security of these systems as these can be beneficial to both the cloud providers and the clients. Although cloud computing offers a lot of benefits, it is very susceptible to security threats which is one of the reasons that some businesses and organizations are hesitant to adopting it. Cloud computing can be vulnerable to security attacks which includes but not limited to misconfigured cloud storage, insecure APIs, poor access control, HTTP-DoS and XML-DoS attacks, virtualization/hypervisor vulnerabilities, compliance violations and regulatory actions, and cloud outages. Though there are many vulnerabilities affecting cloud services, the focus of this literature review will be on improving cloud security with emphasis on secure APIs. This study offers a bibliometric analysis that explores the solution to cloud security challenges by systematic review of existing literature on cloud security with focus on securing APIs which would enhance business enterprises in the USA. This literature review will include comparing various works from different authors including books, conference materials, articles, other literature reviews, empirical studies and scientific journals within the last 21 years to provide a comprehensive look within the context of this topic. The work utilized the steps in bibliometric analysis to examines the challenge associated with cloud security by reviewing 24 articles in the cloud security related areas such as cloud security challenges, cloud security privacy, cloud security threats, cloud security alliance, cloud security encryption, cloud security cryptography, cloud security issues and challenges, cloud security virtualization. This study established bibliometric analysis steps and applied statistical analysis tool towards enhancing cloud security by using secured APIs.

I. INTRODUCTION

Cloud computing is transforming the way people consume and manage information technology (IT). It offers cost savings, faster time-tomarket, and the flexibility to scale applications on demand. While the excitement developed tremendously throughout 2008 and has remained subsequently, the author Gartner believes that there is a huge shift towards the cloud computing model and that the advantages might be significant (Gartner, 2021). However, because the cloud computing model is still evolving both conceptually and practically, legal, economic, service quality, interoperability, security, and privacy issues remain key obstacles in cloud computing.

The world's computing infrastructure is quickly transitioning to cloud-based design. While it is critical to take advantage of cloudbased computing by deploying it in a variety of industries, security in a cloud- based computing environment remains a top priority. A new business trend based on cloud technology has emerged as a result of the expansion of cloud-based services and service providers. Sensitive information from various entities is typically stored on remote servers and locations, with the risk of being exposed to unauthorized parties if the cloud servers storing that information are compromised. With the introduction of numerous cloud-based services and geographically distributed cloud service providers, sensitive information from various entities is typically stored on remote servers and locations with inherent high risk of unauthorized access to information. The flexibility and advantages that cloud technology has to offer will have little value if security isn't reliable and consistent. This study is intended to enhance cloud security by using secure APIs in business enterprises in the USA. However, the current objective is to carry out methodical literature review in the area of cloud services and security with a view to appraise each work. Hence, previous studies will be reviewed to highlight the focus or strength of the research, limitations, common findings, and gaps to be filled or areas to be researched in the future.

II. REVIEW METHODOLOGY

2.0 Search process

This study was done using documents indexed by Google scholar database. Google scholar database is a web search engine that searches scholarly articles and journals from different sources and present same to the user based on search keywords, authors, year of publication and other parameters with a combination of Boolean operators for filtering. Google scholar covers an estimate of about 100 million scholarly documents that is written in English language. Some of these documents indexed in google scholars includes peer- reviewed online academic journals, empirical studies, conference papers.

This publication is licensed under Creative Commons Attribution CC BY. https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14531

A systematic literature review was used, with a clearly stated purpose, research question, a defined search approach alongside a comprehensive scientific database to answer our research questions. The Bibliometric analysis for this work focused on co-author, co-word and citation clusters and connection links. For this review, the focus was on books, conference proceedings, articles, other literature reviews and scientific journals within the last 21 years to answer the research questions and analyze the relevant data efficiently. Google scholar uses search methodology like web crawler which is helpful in exclusion of articles not needed in the search results. It is very helpful in identifying journal titles and authors associated with their research topics or area of interest. It is also useful in finding or identifying articles or conference proceedings that would not be found in other indexing services or databases. It is relatively important to note that google scholar uses keywords to search for documents not metadata. Materials from other databases like Research direct, IEEE, Research gate and open access repository of electronic preprints and post prints were also used.

2.1 Research Questions

There are some questions that would be explored in this research that relates to this topic. These questions aim to give an understanding of what to expect in this area of research and will help define the objective of this research. we conducted a systematic examination of the literature in the most comprehensive scientific database, Google scholar to answer the following questions which are:

- How do security challenges affect the adoption of cloud computing?
- What effect does an insecure APIs have on the cloud computing for business enterprises?

These questions will serve as a guide as we review journals, conference papers, and articles on how to address the issue of cloud security in business enterprises with our primary focus to be companies located in the United States. The google scholar database search engine that we will use for this research will gather or pull data from various databases like IEEE, Elsevier, Research direct, Research Gate, arxiv.org

2.2 Article Collection

In November of 2021, we started conducting the search using google scholar database as a literature source starting from the year 2000 till 2021. To find our target publications based on the topics of interest, we used keyword selection which we defined as the sets of keywords to find the documents that is relevant to our research and we identified the publications that would be relevant to our research. Some of those keywords are:

- "Cloud computing framework" which generated 1,480, 000 search results
- "Cloud Computing Overview" which generated 1,170,000 search results
- "Cloud Computing Concepts" which generated 800,000 search results
- "Cloud Computing security challenges" which generated 599,000 search results.
- "Solutions in cloud computing security issues" which generated 458,000 search results
- "Business perspective cloud computing" which generated 452,000 search results
- "Cloud computing and business enterprises" which generated 108,00 search results.
- "Insecure APIs and cloud computing" which generated about 14,100 search results

In part a) the cloud computing when I typed in the selected keyword, 1,480,000 search results were generated including cloud computing framework for service robots were generated. I picked the articles I needed and further narrowed my search in part b) to cloud computing overview which generated 1,170,000 search results. Since I needed to understand the concept and architecture of cloud computing including how it works, I narrowed my search to "Cloud Computing concepts" which generated about 800,000 search results in part c). To further narrow my research and choose the area of concentration for my topic, I decided I wanted to explore the security challenges that cloud computing faces, so I typed in the keyword "Cloud Computing security challenges" in part d) which resulted in 599,000 search results. I further narrowed this search using the keyword "Solutions in cloud computing security issues" result in part e) which resulted to 458,000 searches. Since the scope of my topic focuses on the business enterprises in the USA, I wanted to understand the business perspective of cloud computing which brought my search in part f) to 452,000 search results. Using the AND keyword in "Cloud computing, I needed journals or articles that covered both this topic, so I further narrowed my search using the keyword: "Insecure APIs and cloud computing" which generated 14,100 search results. Out of the 14,100 articles, I filtered out the articles by identifying the most closely related literature to my topic. I excluded duplicated articles or reports, informal literature surveys, and all the articles I did not need which brought my search results I chose, I used 34 for this research. Out of the 34 articles, I picked 24 of them that stood out to be the most interesting and reviewed them extensively in this research.

2.3 Conception and Extraction

We studied published documents by author, title, year, methodology, the strength of the research, limitations, and potential future research areas of all we have gathered so far. We gathered different papers and publications from different countries or regions, analyzed and drew the common findings including any discrepancies we have noticed in any authors' work.

Step 1	 Research Objective What is the research question and the outcome
Step 2	 Research Design Bibliometric analysis with what type of data
Step 3	 Content of Bibliometric Data How to search, Journal based, keyword based etc
Step 4	 Methodology and software which Bibliometric approach and software to choose
Step 5	 Analysis and Result Articles, Institutions and Journals
Step 6	 Findings and interpretations Are research questions answered and guide for future research

Figure 1: The Steps in Literature Review using Bibliometric Analysis

The Bibliometric analysis for literature review has six iterative steps as shown in figure 1. The step 1 focuses on the research objective and what the outcome of the review will look like when completed. The step 2 focuses on research design, the focus of this step is to determine, the type of data to be used for the analysis while step 3 tries to capture the content of the bibliometric data should be included in the review. This includes the search methods, types of scholarly documents to be used among others. In step 4 we pick Bibliometric approach and make selection for the right software based our what our expected outcome should be. In step 5 we do the analysis and present our report. We conclude in step 6 by interpreting the results of our findings which should help in answering the research question we asked while starting the process.

III. DATA ANALYSIS AND PRESENTATION

3.0 Distribution of publication

This review used scholarly papers released between year 2000 and 2021 on Cloud security to provide wider coverage for the analysis of secure APIs and cloud security. Following the steps outlined in figure 1, the process was started and although there have been increase in the number of papers released as the year progressed. The arrival of Covid-19 has forced Enterprises to move to the cloud and continue their business operations as a result, there has been a surge in the cloud adoption since 2019 till date.

3.1 Data Visualization of publication

3.1.1 Keyword Density Analysis

The keyword density is the percentage of times a word appeared compared to the total number of words used in the document and the number of cluster those keywords are connected to. A color band is used to represent the density, clustering and links associated with a keyword as shown in figure 2a.

	cloud ready	cloudusing iso standard application	udy cloud wrt
	cloud security service		survey
	system	colla cloud security	porative cloud cami
	access controls	cloud database secur	access control framework cryptdb ity issue
	challenges	method cloud	cloud storage
	cloud computing platform	azure platform & its cogn	tive rest api access control
A VOSviewer	mobile (cloud behalf cloud provider	android application

Figure 2a: Keyword Density Analysis

3.1.2 Keyword Network Analysis

The VOSviewer was used to create a map for the keywords as shown in figure 2b. The summary result showed Network visualization for keyword having Items: 82, Cluster: 26, Links: 87, The top 5 keywords are presented in table 1.



Figure 2b: Network Visualization of Keyword Density

S/N	Items	Cluster	Link	Occurrences
1	challenges	21	1	3
2	systems	1	5	3
3	Cloud computing platform	3	4	2
4	Mobile cloud	7	3	2
5	rest API access control	8	3	1

Table 1: Top 5 keywords from Network Visualization of Keywords

3.1.3 Network Visualization for cross citation

After the analysis of the bibliographic coupling of citation references, the corresponding network visualization was constructed as shown in the figure 3. The one in red is the parent from which all other citations were derived. Over the years more people doing related research in the field of Cloud security has referenced it, this has 7 clusters and 69 links with each cluster showing a different color for identification and area of research specialization.



Figure 3: Network Visualization of Cloud Security cross citation

3.1.4 Network Visualization for co-author citation

After the analysis of the bibliographic coupling of co-author citation references, the corresponding network visualization was constructed as shown in the figure 4.

The result from the co-author citation showed the summary result as Items: 143, Cluster: 58 and links: 169. The title with highest rating is: SEAPP: A secure application management framework based on REST API access control in SDN-enabled cloud environment, with the following parameters Cluster 1, Links 7, documents: 1.



Figure 4: Network Visualization of co-author citation

3.2 Cloud security challenges

Security problems in cloud computing have been the subject of multiple researches from various perspectives. Jarabek discussed the advantages and disadvantages of virtualization in the cloud (Jarabek, 2011). He also investigated the side-channel data leakage, which are especially dangerous in a virtualized cloud environment, as well as security audits and cloud management. Wang Cong presented a strategy for integrating storage accuracy insurance with data error localization (Wang et.al, 2009). Ian Foster linked cloud computing to grid computing based on numerous findings. The suggested approach is very efficient and durable in the face of Byzantine failure, malicious data alteration assaults, and even server collusion (Foster et. al, 2008). From the perspectives of network, application, and data storage, Rohit explored different security challenges for Cloud computing environments and provided some solutions (Bhadauria et al., 2012).

Jaydip Sen has done some studies in Security and Privacy Issues in Cloud Computing (Sen, 2021). In his work, he described various service and deployment models of cloud computing and identified major challenges with each model. He discussed and suggested some solutions to mitigate those challenges; He concluded his work on a proposal of future trends in cloud computing deployment (Sen, 2021). Kuyoro S. O et-al presented a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types (Kuyoro S. O et. al, 2011).

Based on the Australian Government report on Cloud Computing Security, their study will aid agencies in performing a risk assessment to examine the viability of employing cloud computing services (Australian Government, 2011). Their research gives an outline of cloud computing and its advantages. Most significantly, they produced a set of thought-provoking questions to assist organizations in better understanding the hazards associated with cloud computing. Performing a risk assessment can assist senior corporate executives in determining if cloud computing is sufficient for meeting their business goals while posing an acceptable amount of risk (Australian Government, 2011). The following aspects were covered in their research: data availability and business functioning, data protection from illegal access, and addressing security breaches.

3.3 Trusted Cloud Computing with Secure Resources and Data Coloring

In 2010, Kai Hwang and Deyi Li carried out experiment on Trusted Cloud Computing with Secure Resources and Data Coloring (Hwang & Li, 2010). The research was focused on using Data Coloring and Software Watermarking to provide privacy, security, and copyright in a cloud computing environment (Hwang & Li, 2010). The study's drawback was that Internet clouds need the internationalization of operating and security standards. Interoperability and meshing of clouds are unsolved issues. When it comes to improving federated cloud services, cloud security infrastructure and trust management will be crucial. Privacy, and security in a cloud computing environment is a tiny percentage of what is needed to comprehensively protect the cloud technology, therefore more studies required in other areas of cloud security.

3.4 The State of Public Infrastructure-as-a-Service Cloud Security

In 2015, Wei Huang et al, conducted a survey on "The State of Public Infrastructure-as-a-Service Cloud Security". The security of public IaaS clouds was the subject of this analysis. The customer's confidence in the Cloud Service Provider (CSP) to offer services honestly and accurately is inextricably linked to their use of the cloud (Huang et al., 2015). Customers also trust the CSP to secure their data from other CSP clients, given that public cloud customers are wary of one another. Problems like recognizing and dealing with malicious VM images exist and presently, there are no answers to resolve that in business or academia. There is a lack of standardization in the implementations of cloud control stacks. Mutual trust between cloud ISP and customers in a cloud computing environment is a tiny percentage of what is needed to comprehensively protect the cloud technology.

3.5 Research on Cloud Computing Security Problem and Strategy

Wentao Liu conducted experimental research in 2012 on Cloud Computing Security Problem and Strategy (Liu, 2012). The work was experimental in nature, it concentrated on cloud fundamentals and highlighted cloud characteristics including scalability, elasticity, platform independence, low cost, and dependability. It addressed data privacy as a key security risk for the cloud computing environment since it is heavily reliant on the network and server. The issue of data privacy has stymied the growth of cloud computing, and this security issue is the main barrier to more people migrating to the cloud. To properly handle these difficulties, Cloud computing companies must take all necessary precautions to secure their clients' security.

3.6 A Survey of Research on Cloud Robotics and Automation

A survey conducted by Ben Kehoe, Sachin Patil, Pieter Abbeel, and Ken Goldberg, in 2014, titled "A Survey of Research on Cloud Robotics and Automation (Kehoe et al., 2015)." The research work focused on using the Cloud for robotics and automation systems where Robots handles almost all aspect of activities performed in the cloud. The connectivity intrinsic in the Cloud sparked a slew of privacy and security concerns. Some of these concerns includes data created by Cloud-connected robots and sensors because they might include photographs or video, as well as data from private houses or business trade secrets. Cloud Robotics and Automation opens the possibility of remote attacks on robots and systems: a hacker may take control of a robot and use it to disrupt operation or inflict damage. There is need to have a more stringent policy on cloud connectivity, privacy, and security.

3.7 Quantitative Reasoning About Cloud Security Using Service Level Agreements

The authors Jesus Luna, Ahmed Taha, Rubern Tapero and Neeraj Suri conducted an experiment in 2015 on Quantitative Reasoning about Cloud Security using Service Level Agreements (Luna et.al, 2017). To quantitatively analyze the security level supplied by Cloud

security level agreements (secSLAs), the study effort expanded two state-of-the-art security assessment techniques: Quantitative Policy Trees (QPT) and Quantitative Hierarchy Process (QHP) (Luna et.al, 2017). The absence of real-world data (including standards and best practices) required to experimentally test these advanced concepts will be a significant hurdle to overcome. For instance, through the Cloud Security Alliance's Cloud Service Providers (CSP) community, extensions to QPT and QHP are required in order to incorporate sophisticated security metrics and Cloud secSLA principles such as uncertainty, end-to-end security evaluation (CSP composition), and interdependence among secSLA components such as controls and service level objectives (SLOs).

3.8 Cloud security defense to protect cloud computing against HTTP-DoS and XML-DoS attacks

Ashley Chonka, Yang Xiang, Wanlei Zhou, and Alessio Bonti experimented on Cloud security defense to protect cloud computing against HTTP-DoS and XML-DoS attacks (Chonka et al., 2011). The work on service-oriented architecture and the security application to cloud computing were covered in this study. It also highlighted two threats to cloud systems that are extremely dangerous: H-DoS and X-DoS attacks (Chonka et al., 2011). If one of these attacks hits the cloud, a large company like Amazon EC2 might be crippled. The academic research and industry are moving towards cloud computing. According to the study, the research found the cloud computing security problem to be the same mistakes that were made with the development of the internet (Chonka et al., 2011). These errors were due to a prioritization of functionality and efficiency over security. Security should be designed in tandem with functionality and speed. There is urgent need for cloud computing policy and decision makers to release a framework that makes cloud computing security to be considered and implemented alongside functionality and performance.

3.9 A Cloud Security Assessment System Based on Classifying and Grading

The joint research by Xuexiu Chen, Alibaba Group, Beijing Chi Chen, Chinese Academy of Sciences, Beijing Yuan Tao, Third Research Institute of Ministry of Public Security, Shanghai Jiankun Hu, University of New South Wales, Australia carried out an assessment on "A Cloud Security Assessment System Based on Classifying and Grading" (Chen et al., 2015). To validate the reasonability and validity of the cloud security assessment indicator system, the researchers employed the complete assessment technique. First, the unit assessment determined that the system's safety score is 73 percent, suggesting that the cloud system under consideration poses certain security threats (Chen et al., 2015). The whole attack operation goes undetected, unwarned, and unblocked, indicating that the system's security protection capabilities should be enhanced in the future. According to the findings, a comprehensive cloud security assessment indicator system is required to satisfy the demands of comprehensive cloud security.

3.10 Cloud Computing Adoption Framework (CCAF) – a security framework for business clouds

Cloud Computing Adoption Framework (CCAF) – a security framework for business clouds was an experiment conducted by Victor Chang and his co-authors in 2016 (Chang et al., 2016). The integration of three-layered security: firewall, identity management, and encryption were exhibited in the CCAF security test (Chang et al., 2016). Experiments were designed to demonstrate CCAF multi-layered security as a functional architecture for corporate clouds. CCAF multi-layered can identify and block 9,995 viruses and trojans during penetration tests and can stop over 85 percent of assaults for 100 hours, according to the results (Chang et al., 2016). The major research limitation is the use of viruses and trojans for penetration testing. There is need for collaborators who can provide more up-to-date testing for CCAF and the necessity to try other types of penetration testing to ensure a better coverage of testing results.

3.11 Enhancing cloud security by using hybrid Encryption scheme

The article "Enhancing cloud security by using hybrid Encryption scheme" was a study undertaken in 2015 by Vibhey Bhangotra and Amit Puri (Bhangotra, 2015). The study proposed a system that addresses some of the shortcomings of existing cloud systems. To increase the stability and security of existing cloud systems that utilize symmetric key encryption techniques, new modules were added to the existing system to guarantee data security (Bhangotra, 2015). In cryptographic systems, key management is the most difficult aspect to maintain. There is always the risk of an insider or outsider intrusion on a cloud platform. Employees can obtain or steal keys without the knowledge of end users. The primary purpose is to ensure that data and keys stored in cloud systems are kept private. The work may be expanded to include more efficient secret sharing systems, allowing the proposed system's performance to be enhanced even further. Furthermore, the suggested method may be improved to operate with asymmetric encryption techniques.

3.12 An Overview and Study of Security Issues & Challenges in Cloud Computing

Rajesh Piplode and Umesh Kumar Singh conducted a research titled the "Overview and Study of Security Issues & Challenges in Cloud Computing" (Piplode & Singh, 2012). This study examined cloud computing vulnerabilities, as well as the security challenges that cloud computing poses and the security goals that must be met. Cloud computing security-sensitive applications demands a high level of security and is inherently vulnerable to security breaches (Piplode & Singh, 2012). Therefore, it is necessary to increase bandwidth and capacity, which necessitates a higher frequency and better spatial spectrum reuse (Piplode & Singh, 2012). Another difficult challenge was shown to be large-scale cloud computing. To respond to the demanding requirements of modern networks, they must be made more secure and durable. Cloud computing has a bright future ahead of it, with the prospect of low-cost communications.

3.13 Cloud Computing: Security Issues and Research Challenges

Rabi Prasad Padhy, Dr. Manas Ranjan Patra, and Dr. Suresh Chandra Satapathy, conducted research on Cloud Computing: Security Issues and Research Challenges. This article examined various cloud computing models, security concerns, and cloud computing research problems (Padhi et.al, 2011). The issue of data security is a serious concern in cloud computing. This includes security problems, such as network and virtualization security, all which have been discussed in this research (Padhi et.al, 2011). End-to-end security will be challenging

to implement due to the cloud's complexity. Because cloud computing technology was still in its early stages of development, new security strategies had to be invented, and current security techniques had to be drastically altered to fit with the cloud architecture.

3.14 A Survey on Security Issues in Service Delivery Models of Cloud Computing

In 2011, S. Subashini and V.Kavitha Anna carried out a study on "A survey on security issues in service delivery models of cloud computing" (Subashini & Kavitha, 2011). The research focused on application and data security over the cloud, and it used a framework by which the security methodology varies dynamically from one transaction or communication to another. Many loose ends exist in cloud computing security, scaring away many potential customers. Prospective customers will not be able to maximize the benefits of this technology unless an appropriate security module is in place (Subashini & Kavitha, 2011). This security module should address any concerns that arise from the cloud in all dimensions. To attract potential customers, every aspect in the cloud should be studied at the macro and micro levels, and an integrated solution should be built and delivered in the cloud. For a typical cloud architecture, an integrated security strategy addressing several levels of data security is strongly recommended. By nature, this system is designed to be more dynamic and localized to minimize data insecurity.

3.15 Privacy and Security in Cloud Computing

In 2010, Allan A. Friedman, and Darrell M. West conducted an experiment titled "Privacy and Security in Cloud Computing". This experiment focused on the advantages of cloud computing, such as cost reductions, scalability, and more effective use of IT resources, among other things (Friedman & West, 2010). Cloud computing poses a number of privacy and security problems that must be considered. These hazards aren't all new, and some of them may be minimized through technological investments and client due diligence. Others, on the other hand, are systematic in nature and may not be solved by unilateral invention. Transparency would aid in the selection of a cloud universe that is more security aware. While there will always be some uncertainty in a world of network threats, defined guidelines and coordination among essential parties are strongly recommended to place these platforms on a more secure foundation moving ahead.

3.16 Cloud computing security - data storage and transmission

Cloud computing security - data storage and transmission, was a study carried out by Mrs. C. Theebendra and N. Santhini in 2014. The subject of data security in cloud data storage and transmission, which is fundamentally a distributed storage system, was investigated in this study (Subashini & Kavitha, 2011). An efficient and adaptable distributed approach was presented to secure the accuracy of users' data in cloud data storage (Subashini & Kavitha, 2011). Storage accuracy insurance and data error localization are combined in this system. Instead of employing IPSec or SSL, the presented data transmission technique encrypts data in the upper-layer on top of the transport layer. The experiment showed that the scheme is very efficient and immune to Byzantine failure, malicious data alteration assaults, and even server collusion attacks, thanks to the rigorous security and performance study. Lack of public verifiability and storage correctness assurance of dynamic data and problem of fine-grained data error localization. The cloud security using cryptography is already in use for secure data storage, but it is essential for it to be enhanced for better security in data transmission and storage.

3.17 Cloud computing and security issues in the Cloud

Authors Monjur Ahmed and Mohammad Ashraf Hossain conducted an experiment on Cloud computing and security issues in the Cloud in 2014. The study focuses on cloud computing as a significant potential and profit for both the corporate environment and attackers — each party may benefit from cloud computing in their own way (Ahmed & Hossain, 2014). The immense potential of cloud computing cannot be overlooked just because of security concerns. Because the influence of cloud computing may be seen in both technical and social settings, cloud computing research and associated concerns are not limited to computer issues. Service-oriented architecture and other cloud computing characteristics suggest that the concept of cloud computing would necessitate an examination of its practicality from social, business, technical, and legal perspectives – all of these facets will include security issues in some form, whether technical or strategic (Ahmed & Hossain, 2014). Since cloud computing is destined to become the best (and probably the final) way to corporate computing, it is critical to remove security hurdles as well as other concerns that must be addressed for cloud computing to be more practical for all users.

3.18 Cloud Application Programming Interface Based on REST Framework The authors Vijay. G. R and Dr. A. Rama Mohan Reddy in their research work titled "Cloud Application Programming Interface Based on REST Framework", published by the IJERT(International Journal of Engineering Research & Technology) in 2013 gave a conceptual overview of Cloud API with a focus on REST and SOAP frameworks and how it is important in the public cloud infrastructure particularly SaaS (Software as a Service) and IaaS (Infrastructure as a Service) (G.R & Reddy , 2013). The author conducted an experiment to analyze both REST and SOAP API to see which of them have a better response time in both wired and wireless environments. According to the result of the analysis, REST API have a better response time than SOAP API in both wired and wireless environment in terms of all their functions (GET, POST, DELETE, and PUT) which affects the major performance difference between REST and SOAP (G.R & Reddy , 2013). One of the limitations of this research is the fact that SOAP API was not explored in depth in terms of architecture, functions, and resources like REST API. Although the author stated the reason for this is because REST API is more common among developers and enterprises today for building mobile applications due to it being light in weight unlike SOAP API that is heavyweight. For future research purposes, SOAP frameworks should be explored because it is an integral part of cloud computing in term of web service API. It was also fundamental to building first generation APIs.

3.19 Cloud and Application Programming Interface – Issues and Developments

The authors of this conference paper (Odun-Ayo et al., 2018) wrote a literature review that focuses on the concepts of API and cloud computing. This paper provides a description of cloud computing services and API, its challenges, as well as the trends in API by analyzing the work of different authors from journals, conference papers, reputable magazines, and research papers. The authors defined Cloud computing as a model for enabling a far-reaching, easy, on demand network access to a shared pool of configurable resources which includes

This publication is licensed under Creative Commons Attribution CC BY. https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14531 hardware and software that is used to deliver services to users over the internet (Odun-Ayo et al., 2018). They are three main types of services that the cloud provides which are: SaaS, PaaS, IaaS and each play different roles in cloud computing. With SaaS the cloud providers host software online so that users do not have to bother installing the software on their local machine. Examples of these are your Microsoft, Salesforce.com, and drop box. PaaS services provides an environment for users to develop and display their applications on the web without having to purchase or install any of the software or hardware required for it. Examples are GaE and Microsoft azure. IaaS provides IT infrastructure such as storage, server, and networking resources, and delivers them to organizations that have a subscription via virtual machines that are accessible on the internet (Jadeja and Modi). Examples are DigitalOcean, AWS, Joyent and GoGrid etc. The author discussed the structure of API and how they are divided into four groups namely: web service API (SOAP and REST), Remote calls (SUN RPC, JAVA RMI, and AME), Message passing (AMQP, STOMP), and Application dependent protocols (FTP, SMMP) (Odun-Ayo et al., 2018).

Cloud API can also be vulnerable to injection attacks in which the attacker can send fake APIs command to the application in order to compromise it. The authors mentioned that the solution to preventing this attack is by using sessionless security practices and token-based authentication. In relation to cloud security, although areas of cloud computing such as web application, virtualization, data storage, and Application programming issues were analyzed extensively in the literature review, other core areas such as Identity Management and Access control (IAM) were given very little coverage. IAM is very important to the development of cloud computing in terms of authorizing, managing, and controlling cloud resources to keep enterprise systems secure. Hence, more research ought to be conducted on IAM particularly with how it relates to API security. This is very essential to business enterprises or organizations that rely on cloud services to build their business models and deliver their business solutions.

3.20 API Vulnerabilities in Cloud Computing Platform: Attack and Detection

The article API vulnerabilities in Cloud Computing Platform: Attack and Detection by Mohd Ariffin, Mohd Faisal Ibrahim, Zolidah Kasiran, and Muhammad Azizi discussed about the vulnerabilities of Cloud API and how they make cloud management software vulnerable to attacks such as API exhaustion and authentication Token eavesdropping. The authors described cloud management software as "Software and technologies utilized by public or enterprise organization to build and operate in-house or on-premises cloud platform and infrastructure (Ariffin et al., 2020)." The author described API Authentication services attack as an eavesdropping attack because user credentials such as passwords and other relevant information can be stolen due to the fact that data is communicated in plain text as a way to authenticate users. As a result, this makes the API susceptible to eavesdropping attacks as the token session is not properly encrypted which makes it easier for the packet to be captured during transmission. Hence, user information and passwords are obtained through the authentication token and can be used by attackers to gain user privileges and access other components on the cloud. Another attack described the author is the API request making it difficult for the cloud platform to respond to legitimate API request. Hence, causing it to by crash or by depleting its resources which would hamper the availability of API services.

The authors carried out experiments to simulate an environment to carry out such attacks and use AD3 algorithms to detect such attacks using OpenStack platform as a testbed for these experiments. In detecting the anomalies of API exhaustion attacks and anomalies caused by normal operations from the experiment, a threshold value was put in place to differentiate between these anomalies so as not to mistake normal operation or background traffic as an anomaly. Although the authors discussed how API Exhaustion attacks is carried out and how the attack is detected by identifying anomalies, they did not discuss how to prevent or to mitigate such attacks from occurring in the future. This area of research can be explored for future research purposes along with how to encrypt authentication token to ensure password privacy which is very crucial to secure cloud platforms

3.21 Towards Securing APIs in Cloud Computing

The authors Gunjan, Tiwari and Sahoo in their work "Towards Securing APIs in Cloud Computing" proposes securing APIs through the use of improved Access Control mechanisms. By implementing business rules for access control in the cloud environment such as the principle of least privilege where users will be granted the minimal privilege required to perform one's tasks, least separation of duty which is the process of distributing the responsibilities of tasks among multiple users, delegation of tasks which is assigning a task to another employee when the initial employee is not available to complete that task. The authors mentioned insecure APIs as one of the biggest threats to cloud security, so they focused on implementing the authorization and access control aspect of cloud API to secure the data residing on the cloud and to prevent unauthorized personnel from having access to it (Gunjan et al., 2021).

The authors also addressed the issue of malicious workers that will try to misuse their privileges to manipulate the configuration settings through the cloud API by proposing a model that allows access control policies and authentication mechanisms through the use of Task-Role-Based Access Control model in which users will be granted permissions based through roles and tasks (Gunjan et al., 2021). Once the tasks are completed, the user rights will be revoked. Although the framework proposed by the authors will implement access control mechanisms that will capture the dynamic and ever-changing responsibilities of users unlike the RBAC (Role Based Access Control), other authentication and access control frameworks should be explored as this will provide better security for cloud environments and also open a new avenue for research since the area of Access controls in terms of API security is barely covered.

3.22 Cloud Computing – A Classification, Business Models, and Research Directions

Christof Weinhardt et. al in their work titled Cloud Computing – A Classification, Business Models, and Research Directions, proposed a framework on cloud business model (Weinhardt et al., 2009). While they made a vivid description of models like Cloud and Grid computing, the research focused on Cloud business model framework covering platform, application and infrastructure and classification of Cloud offerings. However, their classifications of cloud services were limited to price model and type of cloud service. Other factors such as functions, usage, business processes, security requirements were not considered for instance looking at scalability and fault tolerance one would be looking at Function-as-a Service (FaaS) (Weinhardt et al., 2009). The reason is because, functions is key requirements in order to ensure that funds are not wasted on inactive resources. The ideal is for user billing to reflect the amount of functionality used. Although the

author mentioned some challenges of Cloud to include security and Cloud API, approach to overcome these issues were missing, therefore a possible research gap of interest to future scholars.

3.23 Cloud computing in the Financial Industry- A Road Paved with Security Pitfalls?

Cloud computing in the Financial Industry- A Road Paved with Security Pitfalls? authored by Ulrich Lampe and Olga Wenge et. al was a research paper delivered during the 18th Americas Conference on Information Systems in August 2012 (Lampe et. al, 2012). The work focused on analyzing of notable security of issues facing cloud computing and its applicability to the financial industry, the effect of security challenges on cloud adoption and applicable risks relating to systems, processes, people, and external context. The review seemingly viewed cloud services as a "perfect match" for the financial industry due to cloud capability to deliver computing power, infrastructure, storage, and applications as utility-like services, but this became doubtful amid security concerns (Lampe et. al, 2012).

Among the security issues listed as impediments to cloud solutions are general security issues, data privacy and governance, monitoring, data migration, communication link, data center etc. The research was carried out by a review using questionnaires and interview and its assessment spanned the ten (10) domains of CISSP with specific objectives to risks that could threaten the Confidentiality, Integrity, and Availability (CIA) of information systems.

However, only two (2) representatives of a certain bank were interviewed in the course of this study, thus, limits the efficacy of the findings. In additional bank is not the only player in the Financial Industry. Although Twenty-Three (23) potential problems and risk that could threaten the security objectives of CIA were identified, details of relevant security measures that could be implemented to mitigate those risks were not discussed. This could form the basis for future studies to wands enhancing cloud security.

3.24 Understanding Taxonomy of Cyber Risks for Cyber Security Insurance of Financial Industry in Cloud Computing

An article which was presented during the 2016 IEEE 3rd International conference on Cyber Security and Cloud Computing, published by IEEE Computer Society in 2016, and captioned "Understanding Taxonomy of Cyber Risks for Cyber Security Insurance of Financial Industry in Cloud Computing" revealed that evolving trends in web-based technology had impacted to a large extent cloud-based business models and solutions (Elnagdy et al., 2016). According to the paper, the evolution invariably led to increasing cyber security risks thereby prompting the advent of Cybersecurity insurance (Elnagdy et al., 2016). Against the backdrop of the growing need for cybersecurity insurance in the financial industry and the attendant cyber concerns inherent in web solutions, the paper engaged a survey approach to review relevant materials with a view to gain insight on the classifications of cybersecurity risks from the cybersecurity insurance perspective; and to create profound awareness of cybersecurity insurance which was targeted towards achieving cost reduction. Cybersecurity incidents, risk management and cyber insurance techniques were found to be critical in managing cybersecurity insurance. While this paper could serve as a useful guide to cybersecurity insurance practice, possible solutions to the identified likely cyber risks were not covered hence a gap that could be explored by future researchers.

3.25 Design and Implementation of Application Programming Interface for Internet of Things Cloud: Design, Implementation of API for IOT Cloud

Design and implementation of application programming interface for internet of things cloud, by Lu Hou et al; published on International Journal Network Management (2016) by John Wiley and Sons Ltd (Hou et al., 2016). The paper discussed in detail the design and implementation of APIs with diverse application protocols for cloud services of internet of things to cushion the effect of scarce resources faced by IoT devices. The work was experimental in nature with a couple of experiments tailored to assess the performance of the intended APIs.

The limitation of the work is the fact that the design and implementation approach of the API was solely performance driven and deployed on Hyper Text Transfer Protocol (HTTP) and Message Queuing Telemetry Transport (MQTT) which provides management functions that enable users manage devices linked to their mobile applications in addition to web app debugging functionalities for developers, all aimed to enhance services for users and effective resource utilization. Security was not considered which exposes the system to risks that could impact on availability. More studies can be conducted on possible ways incorporating security into cloud internet of things while promoting efficiency, reliability, and performance.

3.26

Cloud Computing for Enterprise Architectures

Zaigham Mahmood and Richard Hill (2011) in their research work titled Cloud Computing for Enterprise Architectures had projected that about 14% of all digital information will be stored in the cloud by 2020 (Mahmood & Hill, 2011). The study focused on recognizing clouds offering from enterprise standpoint and as an enabler, enhancing fulfilment of business requirements both for immediate, short, and long-term objectives. According to the authors, Cloud Computing for Enterprise Architectures addresses the need for a single point of reference for state-of-the-art cloud solutions design and implementation techniques (Mahmood & Hill, 2011).

The work was set to determine the current state of developments, ideas, and features in Cloud Computing models, frameworks, technologies, and applications as it relates to engaging cloud services in Enterprise Architecture to facilitate and support evolving business models. In addition to discussing the concepts and principles of Cloud Computing and Enterprise Architecture, frameworks, and methodologies for cloud adoption, as well as issues and challenges with Cloud Computing were presented. Among the key issues raised in the study were data governance and management, availability and reliability of systems and infrastructure, process monitoring and control, service management and data security. Experiments and result analysis was the research methodology employed.

Although the study revealed cloud solutions to be a global trend that has the potentials of massive growth in the area of information and communication technology, more studies need to be done in improvement of existing technologies and introduction of new ones in order to improve scalability, security and availability for faster and wider adoption of cloud services.

IV. CONCLUSION

Common findings revealed that data security is major issue for Cloud Computing and adoption of cloud services will peak if robust and resilient security is built into cloud infrastructure to offer integrated security measures such as secure API, DDOS solutions, behavioral monitoring Solution, and many others, to control threats to cloud security

Cloud computing is inherently vulnerable to cybersecurity attacks; therefore, cloud solutions require high degree of security especially when critical applications are hosted in the cloud. Though the benefits of using cloud computing include potential cost savings, cloud adoption is not yet optimized as cloud computing security has lot of loose ends which discourage many potential users, However the covid-19 has boasted the adoption of cloud technology across various regions. Covid-19 has boasted Enterprise's adoption of cloud technology as seen from the hike in cloud technology deployment since 2019.

Major observations showed great opportunities are associated with cloud computing. Cloud computing models, frameworks, and technologies support evolving business models, however, risks to privacy and security from cloud computing cannot be ignored. Insecure APIs had been mentioned as one of the most common security challenges in cloud computing alongside with data breaches, data loss, and Denial-of- Service Attacks, hence the need to enhancing cloud security by using secure APIs.

One of the areas that were not extensively covered in most of literatures that were reviewed is IAM (Identity Access Management). But this can serve as an opportunity to be studied extensively in the future. In conclusion, there is not much disparity between all the literature review in terms of securing cloud security systems. Most of the literatures were very similar to each other in terms of cloud computing concepts and the vulnerabilities affecting the cloud which is data privacy and security.

TABULAR SUMMARY OF LITERATURE REVIEW

S/N	Author I	Date	Title of	Metho	Strength of research	Common	Limitations of	Gap to be filled
	C C	of	Work	dology		Findings	research	(Potential
	I	Publ						Research Areas)
	i	cati						
	0	<u>n</u>				~ ~ ~		
1	Kai Hwang ²	2010	Trusted	Experi	The research was focused	Common findings	The study's	Privacy and
	University of		Cloud	ment	on using Data Coloring	revealed that data	drawback was that	security in a cloud
	Southern		Computing		and Software	security is major	Internet clouds need	computing
	California		with Secure		Watermarking to provide	issue for Cloud	the	environment is a
	Deyi Li		Resources		privacy, security, and	Computing and	internationalization	tiny percentage of
	Isinghua		and Data		copyright in a cloud	adoption of cloud	of operating and	what is needed to
	University,		Coloring		computing environment.	services will peak	security standards.	comprehensively
	China					if robust and	Interoperability and	protect the cloud
						resilient security is	meshing of clouds	technology.
						built into cloud	are unsolved issues.	
						infrastructure to	When it comes to	
						offer integrated	improving federated	
						security measures	cloud services, cloud	
						such as secure API,	security	
						DDOS solutions,	infrastructure	
						benavioral	and trust	
						monitoring	management will be	
		015		C		Solution, and many	crucial.	Marta 1 tarat
2	Wei Huang,2	2015	The State of	Survey	The security of public laas	others, to control	Problems like	Mutual trust
	Afshar		Public		clouds was the subject of	threats to cloud	recognizing and	between cloud ISP
	Ganjali,		Infrastructure		this analysis. The	Security Cloud commuting	dealing with	and customers in a
	Beom Heyn		-as-a-Service		customer's confidence in	cioua computing	malicious VM	cloud computing
	Kim, Sukwon		Cloud		the Cloud Service	is innerently	images exist and	environment is a
	OH, and		Security		Provider (CSP) to offer	vullerable to	presently, there are	uny percentage of
	David Lie,				services nonestry and	cybelseculity	that in husiness or	what is needed to
					linked to their use of the	allacks, increase,	unat in dusiness or	comprehensivery
					aloud [12] Customer	roquiro high dogroo	acadenna.	protect the cloud
					cloud [12]. Customers	of	There is a last of	technology.
					also trust the CSF to	or security	standardization in	
					sther CSD alignts given	especially when	implementations of	
					that public cloud	applications are	cloud control stocks	
					customors are wary of one	hosted in the cloud	ciouu control stacks.	
					another	Though the		
3	Wentao Liu	2012	Research on	Experi	The study concentrated on	benefits of using	The issue of data	To properly handle
5	wentao Liu 2	2012	Cloud	ment	cloud fundamentals and	cloud computing	nrivacy has stymied	these difficulties
			Computing	mem	highlighted cloud	include potential	the growth of cloud	Cloud computing
			Security		characteristics including	cost savings, cloud	computing and this	companies must
			Problem and		scalability elasticity	adoption is not vet	security issue is the	take all necessary
			Strategy	1	platform independence	optimized as cloud	main barrier to more	precautions to
			Strategy		low cost and	computing security	neonle migrating to	secure their clients'
					dependability. It	has lot of loose	the cloud.	security.
					addressed data privacy as	ends which		security.
					a key security risk for the	discourage many		
					cloud computing	potential users		
					environment since it is	Major observations		
1					heavily reliant on the	showed great		
					network and server.	opportunities are		

4	Ben Kehoe,2014	A Survey of survey	The research workassociated with The connectivity There is need to
	Sachin Patil,	Research on	focused on using the cloud computing. intrinsic in the Cloudhave a more
	Pieter	Cloud	Cloud for robotics and Cloud computingsparked a slew ofstringent policy on
	Abbeel, and	Robotics and	automation systems wheremodels, privacy and security cloud connectivity,
	Ken	Automation	Robots handles almost all frameworks, and concerns. Some of privacy, and
	Goldberg		aspect of activitiestechnologies these concernssecurity
			performed in the cloud. support evolving includes data created
			business models, by Cloud-connected
			however, risks torobots and sensors
			privacy and due to the fact that
			security from cloudthey might include
			computing cannotphotographs or
			be ignored video, as well as data
			Insecure APIs hadfrom private houses
			been mentioned asor business trade
			one of the mostsecrets. Cloud
			common securityRobotics and
			challenges in cloudAutomation opens
			computing the possibility of
			alongside with dataremote attacks on
			breaches, data loss, robots and systems: a
			and hacker may take
			Denial-of-Service control of a robot and
			use it to disrupt
			operation or inflict
			damage.

5	Jesus Luna, Ahmed Taha, Ruben	2015	Quantitative Reasoning About Cloud	Experi ment	To quantitatively analyze the security level supplied by Cloud security level	Attacks, hence the need to enhancing	The absence of real- world data	. Extensions to QPT and QHP are
	Trapero, and NeeraiSuri		Security Using Service		agreements (secSLAs), the study effort expanded	using secure APIs.	and best practices) required to	incorporate sophisticated
	- · · · · · · · · · · · · · · · · · · ·		Level		two state-of-the-art		experimentally test	security metrics
			Agreements		security assessment		these advanced	and Cloud secSLA
					techniques: Quantitative		concepts will be a significant burdle to	principles such as
					Ouantitative Hierarchy	l r	overcome for	to- end security
					Process (OHP).		example, through the	evaluation (CSP
							Cloud Security	composition), and
							Alliance's Cloud	interdependence
							Service Providers	among secSLA
							(CSP) community.	components such
								as controls and
								service level
								(SLOs)
6	Ashlev	2011	Cloud	Experi	The work on service-		The academic	There is urgent
_	Chonka,	-	security	ment	oriented architecture and		research and industry	need for cloud
	Yang Xiang,		defence to		the security application to		are moving towards	computing policy
	Wanlei Zhou,		protect cloud		cloud computing were		cloud computing.	and decision
	Alessio Bonti		computing		covered in this study. It		According to the	makers to release a
			against		also highlighted two		study, the research	framework that
			and XMI		that are extremely		computing security	computing
			DoS attacks		dangerous: H-DoS and X-		problem to be the	Security to be
					DoS attacks. If one of		same mistakes that	considered and
					these attacks hits the		were made with the	implemented
					cloud, a large company	r	development of the	alongside
					like Amazon EC2 might		internet. These errors	functionality and
					be crippled.		were due to a	performance.
							functionality and	
							efficiency over	
							security. Security	
							should be designed	
							in tandem with	
							functionality and	
7	Vuoviu Chon	2015	A Cloud	1	To volidato tha		speed. The whole etteck	According to the
/	Alibaba	2013	A Cloud	Assess	reasonability and validity		operation goes	findings a
	Group.		Assessment	mem	of the cloud security	,	undetected.	comprehensive
	Beijing Chi		System Based		assessment indicator		unwarned, and	cloud security
	Chen,		on		system, the researchers	5	unblocked,	assessment
	Chinese		Classifying		employed the complete		indicating that the	indicator system is
	Academy of		and Grading		assessment technique.		system's security	required to satisfy
	Sciences,				First, the unit assessment		protection	the demands of
	Deijilig Yuan Tao				system's safety score is 73		be enhanced in the	comprehensive
	Third				percent. suggesting that		future.	cioud security.
	Research				the cloud system under	•		
	Institute of				consideration poses	5		
	Ministry of				certain security threats.			
	Public							
	Security,Shan							
	gnai Lionkun Hu							
	University of							
	New South							
	Wales,							
	Australia							

This publication is licensed under Creative Commons Attribution CC BY. https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14531

	000100						
8	Victor Chang,	2014	Cloud	Experi	The integration of three-	The major research	There is need for
	Yen-Hung		Computing	ments	layered security: firewall,	limitation is the use	Collaborators who
	Kuo, Muthu		Adoption		identity management, and	of viruses and trojans	can provide more
	Ramachandra		Framework		encryption were exhibited	for penetration	up-to-date testing
	n		(CCAF) – a		in the CCAF security test.	testing.	for CCAF. There is
			security		Experiments were		an urgent need to
			framework		designed to demonstrate		try other types of
			for business		CCAF multi- layered		penetration testing
			clouds		security as a functional		to ensure a better
					architecture for corporate		coverage of testing
					clouds. CCAF multi-		results.
					layered can identify and		
					block 9,995 viruses and		
					trojans during penetration		
					tests and can stop over 85		
					percent of assaults for 100		
					hours, according to the		
					results.		
9	Vibhey	2015	Enhancing	Experi	The study proposed a	In cryptographic	The work may be
	Bhangotra,		cloud security	ment	system that addresses	systems, key	expanded to
	Amit Puri.		by using		some of the shortcomings	management is the	include more
			hybrid		of existing	most difficult aspect	efficient secret
					cloud systems. To	to	sharing systems,
					increase		

			Encryption		the stability and socurity	maintain Thara is	allowing the
					the stability and security	maintain. There is	anowing the
			scheme		of existing cloud systems	always the risk of an	proposed system's
					that utilize symmetric key	insider or outsider	performance to be
					encryption techniques	intrusion on a cloud	enhanced even
					now modulos woro addad	platform Employees	furthor
					new modules were added	plationin. Employees	
					to the existing system to	can obtain or steal	Furthermore, the
					guarantee data security.	keys without the	suggested method
						knowledge of end	may be improved
						users. The primary	to operate with
						purposa is to ansura	osymmetric
							asymmetric
						that data and keys	encryption
						stored in cloud	techniques.
						systems are kept	
						private.	
						L	
10	Daiach	2012	An Overnier		This study systeminad	Thanafana it ia	To mananal to the
10	Rajesh	2012	All Overview		This study examined	i neretore, it is	To respond to the
	Piplode,		and Study of		cloud computing	necessary to increase	demanding
	Umesh		Security		vulnerabilities, as well as	bandwidth and	requirements of
	Kumar Singh		Issues &		the security challenges	capacity, which	modern networks,
	C		Challenges in		that cloud computing	necessitates a higher	they must be made
			Cloud		nosos and the socurity	frequency and better	more secure and
					poses and the security	inequency and better	nore secure and
			Computing		goals that must be met.	spatial spectrum	durable. Cloud
					Cloud	reuse. Another	computing has a
					computing security-	difficult challenge	bright future ahead
					sensitive applications	was shown to be	of it, with the
					demands a high level of	large-scale cloud	prospect of low-
					demands a high level of	large-scale cloud	prospect of low-
					security and is innerently	computing	cost
					vulnerable to		communications.
					security breaches.		
11	Rabi Prasad	2011	Cloud	Experi	This article examined	End-to-end security	Since cloud
	Padhy Dr	-	Computing:	ment	various cloud computing	will be challenging	computing
	Manaa		Computing.	mem	various cloud computing	to invalue and door to	to sha ala aya ayaa
	ivianas		Security		models, security concerns,	to implement due to	technology was
	Ranjan Patra,		Issues and		and cloud computing	the cloud's	still in its early
	Dr. Suresh		Research		research problems. The	complexity.	stages of
	Chandra		Challenges		issue of data security is a		development, new
	Satanathy		0		serious concern in cloud		security strategies
	Sumpuny,				computing. This includes		had to be invented
					computing. This includes		
					security problems, such as		and current
					network and virtualization		security techniques
					security, all		had to be
					which have been		drastically altered
					discussed in this research		to
					discussed in this research.		fit mith the sland
							fit with the cloud
<u> </u>							architecture.
12	S. Subashini	2011	A survey on	survey	The research focused on	Many loose ends	For a typical cloud
	and		security		application and data	exist in cloud	architecture, an
1	V Kavitha		issues in		security over the cloud	computing security	integrated security
1	· .150 / 1010		aomuioc III		and it used a framework	computing security,	stratagy addressing
1			service		and it used a framework	scaring away many	sualegy addressing
1			delivery		by which the security	potential customers.	several levels of
			models of		methodology varies	Prospective	data security is
1			cloud		dynamically from one	customers will not be	strongly
			computing		transaction	able to maximize the	recommended By
			Paulo		communication to	benefits of this	nature this evetor
1					long the second se	tenternes of this	hature, this system
					another.	technology unless an	is designed to be
						appropriate security	more dynamic and
1						module is in place.	localized to
						This security module	minimize data
1						should address any	insecurity
1						should address ally	moccurity.
						concerns that arise	
1						from the cloud in all	
1						dimensions. To	
						attract potential	
						customers every	
1	1	1	1	1		rusionicis, Evely	

This publication is licensed under Creative Commons Attribution CC BY. https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14531

JOIN 22.	50 5155					-		
							aspect in the cloud	
							should be studied at	
							the macro and micro	
							levels, and an	
							integrated solution	
							should be built and	
							delivered in the	
							cloud	
13	Allan A.	2010	Privacy and	Experi	This experiment focused		Cloud computing	Transparency
	Friedman,		Security in	ment	on the advantages of cloud		poses a number of	would aid in the
	Darrell M.		Cloud		computing, such as cost		privacy and security	selection of a cloud
	West		Computing		reductions, scalability,		problems that must	universe that is
					and more effective use of		be considered. These	more security
					IT resources, among other		hazards aren't all new	aware. While there
					things.		as some of them may	will always be
							be minimized	some uncertainty
							through	in a world of
							technological	network threats,
							investments and	defined guidelines
							client due diligence.	and coordination
							Others, on the other	among essential
							hand, are systematic	parties are strongly
1							in nature and may	recommended to
							not be solved by	place these
							unilateral invention.	platforms on a
1								more
1								secure foundation
1								

14	Mrs. C.	2014	Cloud	Experi	The subject of data	Lack of public	The cloud security
	Theebendra,		computing	ment	security in cloud data	verifiability and	using cryptography
	N. Santhini,		security - data		storage and transmission,	storage correctness	is already in use for
	, í		storage and		which is fundamentally a	assurance of	secure data storage.
			transmission		distributed storage system,	dynamic data and	but it is essential
					was investigated in this	problem of fine-	for it to be
					study. An efficient and	grained data error	enhanced for better
					adaptable distributed	localization.	security in data
					approach was presented to		transmission and
					secure the accuracy of		storage.
					users' data in cloud data		C
					storage. Storage accuracy		
					insurance and data error		
					localization are combined		
					in this system.		
					Instead of employing		
					IPSec or SSL, the		
					presented data		
					transmission technique		
					encrypts data in the upper-		
					layer on top of the		
					transport layer. The		
					experiment showed that		
					the scheme is very		
					efficient and immune to		
					Byzantine failure,		
					malicious data alteration		
					assaults, and even server		
					collusion attacks, thanks		
					to the rigorous security		
					and performance		
					study.		
15	Monjur	2014	Cloud	Experi	The study focuses on	. Because the	Since cloud
	Ahmed,		computing	ment	cloud computing as a	influence of cloud	computing is
	Mohammad		and security		significant potential and	computing may be	destined to become
	Ashraf		issues in the		profit for both the	seen in both	the best (and
	Hossain,		Cloud		corporate environment	technical and social	probably the final)
					and attackers — each	settings, cloud	way to corporate
					party may benefit from	computing research	computing, it is
					cloud computing in their	and associated	critical to remove
					own way. The immense	concerns are not	security hurdles as
					potential of cloud	limited to computer	well as other
					computing cannot be	issues (Ahmed &	concerns that must
					overlooked just because of	Hossain, 2014).	be addressed for
					security concerns	Service-oriented	cloud computing to
						architecture and	be more practical
						other cloud	for all users.
						computing	
						characteristics	
						The the	
						suggest that the	
						concept of cloud	
						concept of cloud computing would	
						concept of cloud computing would necessitate an	
						concept of cloud computing would necessitate an examination of its	
						concept of cloud computing would necessitate an examination of its practicality from	
						concept of cloud computing would necessitate an examination of its practicality from social, business,	
						concept of cloud computing would necessitate an examination of its practicality from social, business, technical, and legal	
						concept of cloud computing would necessitate an examination of its practicality from social, business, technical, and legal perspectives – all of	
						concept of cloud computing would necessitate an examination of its practicality from social, business, technical, and legal perspectives – all of these facets will	
						suggest that the concept of cloud computing would necessitate an examination of its practicality from social, business, technical, and legal perspectives – all of these facets will include security	
						suggest that the concept of cloud computing would necessitate an examination of its practicality from social, business, technical, and legal perspectives – all of these facets will include security issues in some form,	
						suggest that the concept of cloud computing would necessitate an examination of its practicality from social, business, technical, and legal perspectives – all of these facets will include security issues in some form, whether	

International Journal of Scientific and Research Publications, Volume 14, Issue 1, Januar	ry 2024
ISSN 2250-3153	

16	Wijow	CP	0012	Cloud	Evnori	This research gives on	Pagad on the regult IVE DEST
10	vijay. Dr A	U.K,	2015	Application	Experi	This research gives an	of the analysis it is COAD
	DI. A.	Kaina		Application	ment	overview of cloud API and	of the analysis, it is boAP
	Nonan			Programming		now it is used in cloud	snown that RESI framework should
	Reddy			Interface		platforms particularly	API have a betterbe explored more
				Based or	l	SaaS (Software as a	response time thanin terms of
				REST		Service) and IaaS	SOAP API in bothfunctions,
				Framework		(Infrastructure as a	wired and wirelessarchitecture, and
						Service) to interact with	environment in termsresources for future
						the cloud and provide	of all their functions research purposes.
						services to users and	(GET, POST,
						enterprises. The authors	DELETE, and
						also mentioned how the	PUT) affecting the
						cloud API is divided into	major performance
						two web service API	difference between
						which are SOAP (Simple	REST and SOAP.
						Object Access Protocol)	Although the
						and REST	functionality of
						(Representational State	REST API was
						Transfer) framework with	explored in depth in
						REST API being the most	this research, SOAP
						popular among developers	API should have also
						today. The author	been explored more
						performed an experiment	as well. In as much as
						to compare both APIS to	REST API is more
						see which have a better	popular and
						response time in wired and	preferred among
						wireless environments	developers and
							enterprises for
							building applications
							including mobile
L							menuting moone

						devices. SOAP API	
						framework is an	
						integral part of cloud	
						computing as many	
						first-generation API	
						was written in	
						SOAP.	
17	Isaac Odun-	2020	Cloud and	Literat	The authors of this paper	API in cloud	In order to bridge
- /	Avo	_0_0	Application	ure	focuses on API and cloud	computing has	this gan in this area
	Chinonso		Programming	Review	computing by examining	become a hot topic as	of cloud
	Okereke		Interface –		related works of different	of recent but a lot	computing
	Hope		Issues and		authors from journals	must be uncovered in	identity
	Orovwode		Development		conferences white papers	this area for future	management and
	orovwode		s		etc to give an	research nurnoses in	access control
			6		understanding of API and	terms of security	(IAM) in cloud
					cloud computing as well	concerns For	computing needs to
					as the challenges affecting	instance they are	be studied more
					their potential. This article	seven core areas	among researchers
					focuses on the types of	relevant to cloud	among researchers
					API and cloud computing	computing and API	how it affects or
					arvices trends in ADI	in terms of security	rolatos to ADIs
					current issues affecting the	They are	This is yerv
					socurity vulnerabilities of	virtualization data	assortial to
					A DL as well as their	storago wab	business
					AFI as well as these	storage, web	ousilless
					solutions to those	application,	enterprises or
					discussed the structure of		organizations that
					A DI A DI anglita atawa	programming	rely on cloud
					API, API architectures	interface, identity	their husiness
					deploying on developing	management,	models and deliver
					aloud applications	general security	their husiness
					cioud applications.	concerns and	uleir dusiliess
						machine learning.	solutions.
						Dased on the author a	
						tor of research papers	
						iend to focus on	
						issues related to web	
						application,	
						virtualization, data	
						storage, and	
						application	
						programming issues.	
						General security	
						concerns were giving	
						some coverage to	
						some extent, but	
						Issues related to	
						machine learning	
						and most	
						importantly, identity	
						management were	
1						given very little	
						coverage. Identity	
						Management and	
1						Access control is	
						very crucial to the	
						development of	
						cloud computing in	
1						terms of authorizing,	
						managing, and	
						controlling cloud	
						resources to keep	
						enterprise systems	
						and data secured.	

						1		
							Therefore, it should	
							be discussed the	
							some way and given	
							same way and given	
							the same amount of	
							attention as the other	
							areas	
							areas.	
1.0		2020	A DI	г ·			T 1	A 1.1 1 ···
18	Mohd Faisal	2020	API	Experi	This research focuses on		In detecting the	Although the
	Ibrahim,		Vulnerabilitie	ment	the vulnerabilities of API		anomalies of API	authors discussed
	Muhammad		s in Cloud		in cloud management		exhaustion attacks	how API
	Azizi Mala		Commutine	1	a ftware which if	1	and anomal'	Exhaustion attact
	AZIZI, Mohd		Computing		software which if not		and anomalies	Exhaustion attack
	Ariffin, and		Platform:		properly addressed, it may		caused by normal	is carried out and
	Zolidah		Attack and		lead to security issues and		VM operations from	how the attack is
	Vogiron		Dotoctor	1	moly couldo on interfere	1	the evenemine of	datastad
	Kasiran.		Detection		may cause an interference		uie experiment, a	detected by
					or disruption of cloud		threshold value was	identifying
					services. The authors		put in place to	anomalies but not
					addraggad this is the		differentiete letere	how to more the
					addressed this issue		unierentiate between	now to prevent or
					through an experiment by		these anomalies so as	to mitigate such
					simulating authentication		not to mistake	attacks from
					tokon oowoodronning	1	normal anarctica	
					ioken eavesdropping and		normal operation or	occurring in the
					API exhaustion attack and		background traffic as	tuture. This area
					using AD3 algorithm to		an anomaly. Even	can be explored for
					detect it		though the method of	future recorch
							mough the method of	iuture research
				1	1	1	detection is accurate.	purposes.

This publication is licensed under Creative Commons Attribution CC BY. https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14531

			there	was no	How	to	encrypt
			additiona	l or	packet	and	ensure
			secondary	y source to	passwo	ord	privacy
			confirm t	he accurate	is very	cruc	ial and

						detection of these	should be explored
						anomalies which is	in future research.
						the limitation of this	
						research	
10	V	2012	Tamada	Deces	The such and Coursian	A lab assala dha	The factories
19	Kumar	2013	Towards	Propos	The authors Gunjan,	Although the	The Tramework
	Gunjan, R. K.		Securing	ed a	Tiwari and Sahoo	framework proposed	proposed by the
	Tiwari, G.		APIs in Cloud	Task-	proposes securing APIs in	by the authors will	authors have the
	Sahoo		Computing	based	cloud computing through	implement access	potential to be
				access	the use of improved	control mechanism	beneficial in the
				control	Access Control	that will capture the	area of securing
				model	mechanisms by	dvnamic and ever	APIs in cloud
					implementing business	changing	computing other
					rules such as principle of	responsibilities of	access control
					least privilege separation	users unlike the	frameworks should
					of duty and delegation of	DDAC (Dolo Docod	ha avaland as well
					of duty and delegation of	KDAC (Role Dased	be explored as well
					tasks for access control in	Access Control),	because it opens
					the cloud environment.	other authentication	more opportunities
					The authors mentioned	and access control	for future research
					insecure APIs as one of	frameworks should	work in this area.
					the biggest threats to cloud	be explored as this	
					security.	will provide better	
					The authors proposed a	security for cloud	
					model that allows access	environments and	
					control policies and	also open a new	
					authentication	avenue for research	
					machanisms through the	avenue for research	
					mechanisms unough the	since the area of	
					use of Task- Role-Based	Access controls in	
					Access Control in which	terms of API security	
					users will be granted	is barely covered.	
					permissions based through		
					roles and tasks so as		
					to prevent users from		
					mismanaging their		
					privileges.		
20	Prof Dr	2009	Cloud	Propos	The research focused on	Classification of	Although the
_0	Christof	2007	Computing _	ed a	Cloud business model	cloud services were	author mentioned
	Weinhardt		دomputing ۸	cloud	framework covering	limited to price	some challenges of
	w chinarut,		A Classification	husings	nlatform application and	madel and type of	Cloud to include
				busines	plation, application and	model and type of	Cloud to include
	wirt Arun		, Business	s model	intrastructure and	cloud service	security and Cloud
	Anandasiva,		Models, and	framew	classification of Cloud	(Functions, usage,	API, approach to
			Research	ork	offerings.	business processes,	overcome these
	Dr. Benjamin		Directions			security	issues were
	Blau,					requirements not	missing.
						considered for	
	Nikolay					instance looking at	
	Borissov.					scalability and fault	
	,					tolerance one would	
	Thomas					he looking at FaaS)	
	Moin1					Eurotions is kow	
	1v1C1111,					requirements	
	W7:					requirements in	
	wirt Wibke					order to ensure that	
	Michalk,					tunds are not wasted	
						on inactive	
	Dr. Jochen					resources. The ideal	
	Stößer					is for user billing to	
						reflect the amount of	
						functionality used	
	1					used	

International Journal of Scientific and Research Publications, Volume 14, Iss	sue 1, January 2024
ISSN 2250-3153	

5511 22.	0 0 100					
21	Ulrich	2012	Cloud Case	The work focused on	However, only two	Although Twenty-
	Lampe,		computing instudies	analyzing of notable	(2) representatives of	Three (23)
	Alexander		the Financialand	security of issues facing	a certain bank were	potential problems
	Müller, Olga	L	Industry- Asurveys	cloud computing and its	interviewed in the	and risk that could
	Wenge, Ralf		Road Paved	applicability to the	course of this study,	threaten the
	Schaarschmid	L	with Security	financial industry, the	thus, limits the	security objectives
	t		Pitfalls?	effect of security	efficacy of the	of CIA were
				challenges on cloud	findings. In	identified, details
				adoption and applicable	additional bank is not	of relevant security
				risks relating to systems,	the only player in the	measures that
				processes, people, and	Financial Industry.	could be
				external context.	•	implemented to
				The research was carried		mitigate those risks
				out by a review using		were not discussed.
				questionnaires and		This could form the
				interview and its		basis for future
				assessment spanned the		studies to wands
				ten (10) domains of CISSP		enhancing cloud
				with specific objectives to		security.
				risks that could threaten		·
				the Confidentiality,		
				Integrity, and Availability		
				(CIA) of information		
				systems.		
22	Sam Adam	2016	Understandin Survey	This paper revealed that	Cybersecurity	While this paper
	Elnagdy,		g the	evolving trends in web-	incidents, risk	could serve as a
	Meikang Qiu,	,	Taxonomy of	based technology had	management and	useful guide to
	Keke Gai		Cyber Risks	impacted to a large extent	cyber insurance	cybersecurity
			for Cyber	cloud-based business	techniques were	insurance practice,
			Security	models and solutions.	found to be critical in	possible solutions
			Insurance of	According to the authors,	managing	to the identified
			Financial	the evolution invariably	cybersecurity	likely cyber risks
			Industry in	led to increasing cyber	insurance.	were not covered
			Cloud	security risks thereby	Against the backdrop	hence a gap that
			Computing	prompting the advent of	of the growing need	could be
				Cybersecurity insurance.	 for cybersecurity	

101	511 225	0 5155					
							insurance in the explored by future
							financial industry researchers
							and the effect dent
							and the attendant
							cyber concerns
							inherent in web
							solutions, the paper
							engaged a survey
							engaged a survey
							approach to review
							relevant materials
							with a view to gain
							insight on the
							classifications of
							cybersecurity risks
							from the
							from the
							cybersecurity
							insurance
							perspective: and to
							create profound
							encate protound
							awareness of
							cybersecurity
							insurance which was
							targeted towards
							achieving cost
							reduction
	22	п. т.	2016	During 1	r		The limit diam of the Manual diamond
ł	23	Hou Lou,	2016	Design and	Experi	The paper discussed in	The limitation of the viore studies can
		Xing Li,		Implementati	ment	detail the design and	work is the fact that be conducted on
		Shaohang		on of		implementation of APIs	the design and possible ways
		Zhao, and		Application		with diverse application	implementation incorporating
		Periklis		Programming		protocols for cloud	approach of the APIsecurity into cloud
		Chatzimisios		Interface for		services of internet of	was solelvinternet of things
		enatziinisios,		Internet of		things to such on the effect	norformance driven while promoting
						unings to cushion the effect	performance driven while promoting
				Things cloud:		of scarce resources faced	and deployed onefficiency,
				Design,		by IoT devices. The work	Hyper Text Transferreliability, and
				Implementati		was experimental in	Protocol (HTTP) and performance.
				on of API for		nature with a couple of	Message Queuing
				IOT Cloud		experiments tailored to	Telemetry Transport
						assess the performance of	(MOTT) which
						the intended ADIs	provides
						the intended AF IS.	provides
							management
							functions that enable
							users manage
							devices linked to
							their mobile
							applications in
							addition to web one
							addition to web app
							debugging
							functionalities for
							developers, all aimed
							to enhance services
							for users and
							offactiva resource
							checuve resource
							utilization.
							Security was not
							considered which
							exposes the system
							to risks that could
							impact
							on availability
- 1							

International Journal of Scientific and Research Publications, Volu-	me 14, Issue 1, January 2024
ISSN 2250-3153	

24	Zaigham	2011	Cloud	Experi	The study focused on	In addition to Although the study
	Mahmood		Computing	ment	recognizing clouds	discussing therevealed cloud
	and Richard	l	for Enterprise		offering from enterprise	concepts and solutions to be a
	Hill		Architectures		standpoint and as an	principles of Cloudglobal trend that
					enabler, enhancing	Computing and has the potentials
					fulfilment of business	Enterprise of massive growth
					requirements both for	Architecture, in the area of
					immediate, short, and	frameworks, and information and
					long- term objectives.	methodologies forcommunication
					The work was set to	cloud adoption, astechnology, more
					determine the current state	well as issues and studies need to be
					of developments, ideas,	challenges withdone in
					and features in Cloud	Cloud Computingimprovement of
					Computing models,	were presented.existing
					frameworks, technologies,	Among the keytechnologies and
					and applications as it	issues raised in the introduction of
					relates to engaging cloud	study were datanew ones in order
					services in Enterprise	governance and to improve
					Architecture to facilitate	management, scalability, security
					and support evolving	availability and and availability for
					business models.	reliability of systems faster and wide
						and infrastructure, adoption of cloud
						process monitoringservices.
						and control, service
						management and
						data
						security.

REFERENCES

- [1] Gartner Special Reports | Gartner. (2021). Retrieved 6 December 2021, from http://www.gartner.com/technology/research/hype-cycles/
- [2] Jarabek, C. (2011). A Review of Cloud Computing Security: Virtualization, Side-Channel Attacks, and Management. University of Calgary.
- [3] Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). Cloud Computing and Grid Computing 360-Degree Compared. 2008 Grid Computing Environments Workshop. doi: 10.1109/gce.2008.4738445
- Wang, C., Wang, Q., Ren, K., & Lou, W. (2009). Ensuring data storage security in Cloud Computing. 2009 17Th International Workshop on Quality of Service. doi: 10.1109/iwqos.2009.5201385
- [5] Bhadauria, R., Sanyal, S., Chaki, N., & Chaki, R. (2012). Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. International Journal of Computer Applications, 47(18), 47-66. doi: 10.5120/7292-0578
- [6] Sen, J. (2021). Retrieved 6 December 2021, from https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf
- [7] Kuyoro, S. O. and Ibikunle, F. and Awodele, O. (2011) Cloud Computing Security Issues and Challenges. International Journal of Computer Networks (IJCN), 3 (5). pp. 247-255.
- [8] Australian Government. (2011). Cloud Computing Security Considerations. Australian Cyber Security Centre.
- [9] Hwang, K., & Li, D. (2010). Trusted Cloud Computing with Secure Resources and Data Coloring. IEEE Internet Computing, 14(5), 14-22. https://doi.org/10.1109/mic.2010.86
 - 10) (Hwang & Li, 2010)
- [10] Huang, W., Ganjali, A., Kim, B., Oh, S., & Lie, D. (2015). The State of Public Infrastructure-as-a- Service Cloud Security. ACM Computing Surveys, 47(4), 1-31. https://doi.org/10.1145/2767181
- [11] Liu, W. (2012). Research on cloud computing security problem and strategy. 2012 2Nd International Conference on Consumer Electronics, Communications And Networks (Cecnet). https://doi.org/10.1109/cecnet.2012.6202020
- [12] Kehoe, B., Patil, S., Abbeel, P., & Goldberg, K. (2015). A Survey of Research on Cloud Robotics and Automation. IEEE Transactions On Automation Science And Engineering, 12(2), 398-409. https://doi.org/10.1109/tase.2014.2376492
- [13] Luna, J., Taha, A., Trapero, R., & Suri, N. (2017). Quantitative Reasoning about Cloud Security Using Service Level Agreements. IEEE Transactions on Cloud Computing, 5(3), 457-471. https://doi.org/10.1109/tcc.2015.2469659
- [14] Chonka, A., Xiang, Y., Zhou, W., & Bonti, A. (2011). Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal Of Network and Computer Applications, 34(4), 1097-1107. https://doi.org/10.1016/j.jnca.2010.06.004
- [15] Chen, X., Chen, C., Tao, Y., & Hu, J. (2015). A Cloud Security Assessment System Based on Classifying and Grading. IEEE Cloud Computing, 2(2), 58-67. https://doi.org/10.1109/mcc.2015.34
- [16] Chang, V., Kuo, Y., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, 57, 24-41. https://doi.org/10.1016/j.future.2015.09.031
- [17] Vibhey Bhangotra, A. P. (2015). Enhancing cloud security by using hybrid encryption scheme.
- [18] Piplode, R., & Singh, U. (2012). An Overview and Study of Security Issues & Challenges in Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering, 2(9).
- [19] Padhi, R., Patra, M., & Satapathy, S. (2011). Cloud Computing: Security Issues and Research Challenges. International Journal of Computer Science And Information Technology & Security, 1(2).
- [20] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal Of Network and Computer Applications, 34(1), 1-11. https://doi.org/10.1016/j.jnca.2010.07.006
- [21] Friedman, A., & West, D. (2010). Privacy and Security in Cloud Computing, (3). Retrieved 6 December 2021, from https://www.brookings.edu/wpcontent/uploads/2016/06/1026_cloud_computing_friedman_west.pdf.
- [22] Theebendra, C., & Santhini, N. (2014). CLOUD COMPUTING SECURITY DATA STORAGE AND TRANSMISSION. INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS, 2(2), 27-35.
- [23] Ahmed, M., & amp; Ashraf Hossain, M. (2014). Cloud computing and security issues in the cloud. International Journal of Network Security & amp; Its Applications, 6(1), 25–36. https://doi.org/10.5121/ijnsa.2014.6103
- [24] G.R, V., & Reddy, A. R. M. (2013). Cloud Application Programming Interface Based on REST Framework. International Journal of Engineering Research & Technology, 2(6), 2202–2206
- [25] Odun-Ayo, I., Evwieroghene, O., & Okereke, C. (2018). Cloud and Application Programming Interface Issues and Developments. London, UK; ResearchGate. Retrieved 6 December 2021, from https://www.researchgate.net/publication/333402621_Cloud_and_Application_Programming_Interface.
- [26] G.R, V., & Reddy, A. R. M. (2013). Cloud Application Programming Interface Based on REST Framework. International Journal of Engineering Research & Technology, 2(6), 2202–2206.
- [27] Ariffin, M., Ibrahim, M., & Kasiran, Z. (2020). API Vulnerabilities in Cloud Computing Platform: Attack And Detection. International Journal of Engineering Trends and Technology, 8-14. https://doi.org/10.14445/22315381/cati1p202
- [28] Gunjan, K., Tiwari, R., & Sahoo, G. (2021). Towards Securing APIs in Cloud
- [29] Computing. International Journal Of Computer Engineering & Applications, 2(2), 27-32. Retrieved 6 December 2021, from https://arxiv.org/abs/1307.6649 https://arxiv.org/abs/1307.6649
- [30] Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., & Stößer, J. (2009). Cloud Computing A Classification, Business Models, and Research Directions. Business & Information Systems Engineering, 1(5), 391-399. https://doi.org/10.1007/s12599-009-0071-2
- [31] Lampe, U., Wenge, O., Müller, A., & Schaarschmidt, R. (n.d.). Cloud computing in the Financial Industry- A Road Paved with Security Pitfalls? Retrieved December 6, 2021, from https://core.ac.uk/download/pdf/301356313.pdf.
- [32] Elnagdy, S. A., Qiu, M., & Conference on Cyber Security and Cloud Computing (CSCloud). https://doi.org/10.1109/cscloud.2016.46
- [33] Hou, L., Zhao, S., Li, X., Chatzimisios, P., & amp; Zheng, K. (2016). Design and implementation of application programming interface for internet of things cloud. International Journal of Network Management, 27(3). https://doi.org/10.1002/nem.1936

This publication is licensed under Creative Commons Attribution CC BY. https://dx.doi.org/10.29322/IJSRP.14.01.2024.p14531 [34] Mahmood, Z., & Hill, R. (2011). Cloud computing for enterprise architectures. Springer.

AUTHORS

First Author – Glory