IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

Impact of Cloud Computing in Today's ERA: A Critical Analysis

[1]Ms. Swati Jaiswal and [2]Dr. Tryambak Hiwarkar
Research Scholar, Department of CSE[1]
Professor, Department of CSE[2]
Sardar Patel University Balaghat, MP, India

Abstract: *Cloud computing is a relatively new technology that uses a distributed network of servers and clients to store and process data in real time. It provides users with more options and less overhead by way of scalable, on-demand services at lower costs. New technologies also raise several questions regarding personal safety and confidentiality. Most importantly, cloud computing relies on CIA (Confidentiality, Integrity and Availability). The biggest worry regarding security is the multi-location of private data, the place where the data is to be held, different rules for processing data, and data commotion, in which different categories of data can get mixed up if they are not handled and stored separately. Research is ongoing, and ensuring that sensitive user data and information is kept private is essential for protecting systems from a wide range of well-known dangers. There are many security risks and concerns that cloud computing must address.*

In this paper, we discuss the importance of data security, review the different types of security aspects and concerns, threats, attacks, and vulnerabilities that are affecting the Cloud Computing environment, and identify relevant existing solution directives to strengthen security, privacy, and tools for protecting against the various attacks in the Cloud.

The term "cloud computing" refers to a new computing paradigm in which multiple computers and networks are interconnected in real time. It gives customers more options and requires less investment in infrastructure while providing them with on-demand services that are both affordable and scalable. There are numerous privacy and security concerns that arise along with the advent of new technologies. Cloud computing's primary features are CIA (Confidentiality, Integrity and Availability). The biggest worry regarding security is the multi-location of private data, the site where the data is to be held, the varying regulations for processing data, and the data turmoil in which different categories of data can get mixed up if they are not handled and stored separately. It is a hot topic of study to find ways to protect users' personal information while simultaneously fending off the many threats that are currently at large. Cloud computing faces its own set of security challenges and dangers.

In this paper, we discuss the importance of data security, review and Present the result various aspect of different types of security aspects and concerns, threats, attacks, and vulnerabilities that are affecting the Cloud Computing environment, and then identify pertinent existing solution directives to bolster security, privacy, and tools for protecting against the different attacks that are prevalent in the Cloud.

Keywords: DDos Attack, HTTP Attack, flood attack.

I. INTRODUCTION

The phrase "Cloud Computing" is typically used to market hosted services, or the deployment of application Services that execute client server software at a remote data center. SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service and/or Identity as a Service) are all common abbreviations for this type of service. Business software and user data are stored on remote servers, and end users access these applications through a web browser, thin client, or mobile apps. In Cloud Computing, it is important to pay attention to the following security features:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

- **Confidentiality:** User privacy should be protected in Cloud infrastructures. Physical isolation and encryption are two of the most used methods for maintaining privacy.
- **Integrity:** Data integrity is of paramount importance. The use of digital signatures has become widespread in the assessment of data integrity. Methods like RAID-type schemes, digital signature, and so on provide some promise of making this a reality**.**
- **Availability:** At the precise moment of need, users should be able to get relevant information or data. Hardening and redundancy are two examples of data/information solutions used to increase the availability of Cloud systems and the applications they host.

II. TYPES OF DOS ATTACKS

Distributed Denial of Service Attack: It takes place when numerous systems collaborate to launch a coordinated denial of service assault on a single target. The target of this attack is simultaneously assaulted from a number of different areas.

To put it another way, a DDoS assault takes use of many distinct sources in order to send a large number of packets that contain no useful information to the target in a very short amount of time. This causes the target's resources to be consumed and its services to be unavailable. Attack, and it is also the easiest to execute, the most damaging, the most complex to avoid, and the most difficult to detect.

Now, pretend you're browsing the web and you notice that one of the pages loads a bit slowly. A high volume of visitors to their site might mean that their servers need to be more scalable. Most sites think about this kind of thing in advance. It is possible that they are the target of a DDoS assault, or Distributed Denial of Service. Denial of Service and Prevention

HTTP POST DDoS Attack: During this type of attack, the adversary will submit a full and valid HTTP POST header. This header will contain a field labelled "Content-Length," which will describe the size of the message body. The actual message body is then sent by the attacker at a pace of almost 1 byte every 110 seconds, which is a painfully slow speed. Because the message was complete and accurate, the destination server would attempt to obey the "Content-Length" field in the header by waiting for the entire body of the message to be delivered before continuing on [68]. This would cause the communication to move more slowly.

In order to overload a target server, an HTTP flood assault uses a volumetric distributed denial-of-service (DDoS) technique known as a flood of HTTP requests.

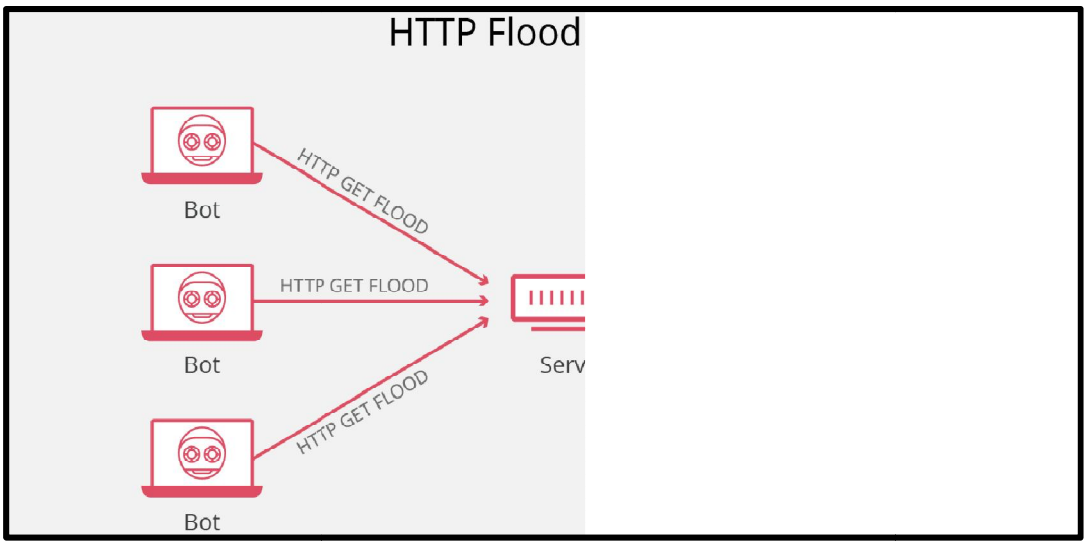

Figure: 1 HTTP Flood Attack

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

FLOOD ATTACKS:

[1,2,3]Hackers can obtain unauthorized access to business systems by exploiting a software coding fault known as a buffer overflow vulnerability. This issue occurs when a program's buffer is larger than its intended size. It is one of the most well-known flaws in software security, although despite its notoriety, it is still very widespread. This is due, in part, to the fact that buffer overflows can happen for a variety of reasons, and the methods that are employed to avoid them are frequently error-prone.

The problem is in the software's handling of buffers, which are regions of memory that are arranged sequentially and used to temporarily store data while it is being moved between places. A buffer overflow is the same thing as a buffer overrun; it happens when the quantity of data in the buffer exceeds the capacity of the storage it has available. This additional data overflows into neighboring memory regions, which then either causes the data in those areas to become corrupted or causes it to be overwritten.

III. PROCEDURE FOR AVERTING DDoS BOUTS

Three distinct forms of filtering are used by our suggested algorithms to thwart DDoS assaults. When the first filter, the second filter, and the third filter are combined, it is powerful enough to stop DDoS assaults. Third parties utilize our primary filter for authentication needs. To ensure a safe transmission of the authentication code, we've opted to employ a third-party authentication service. The second filter we use is based on a comparison between the current requests and an arbitrary maximum number of requests taken from the database. The faked packets are eliminated using the final filter.

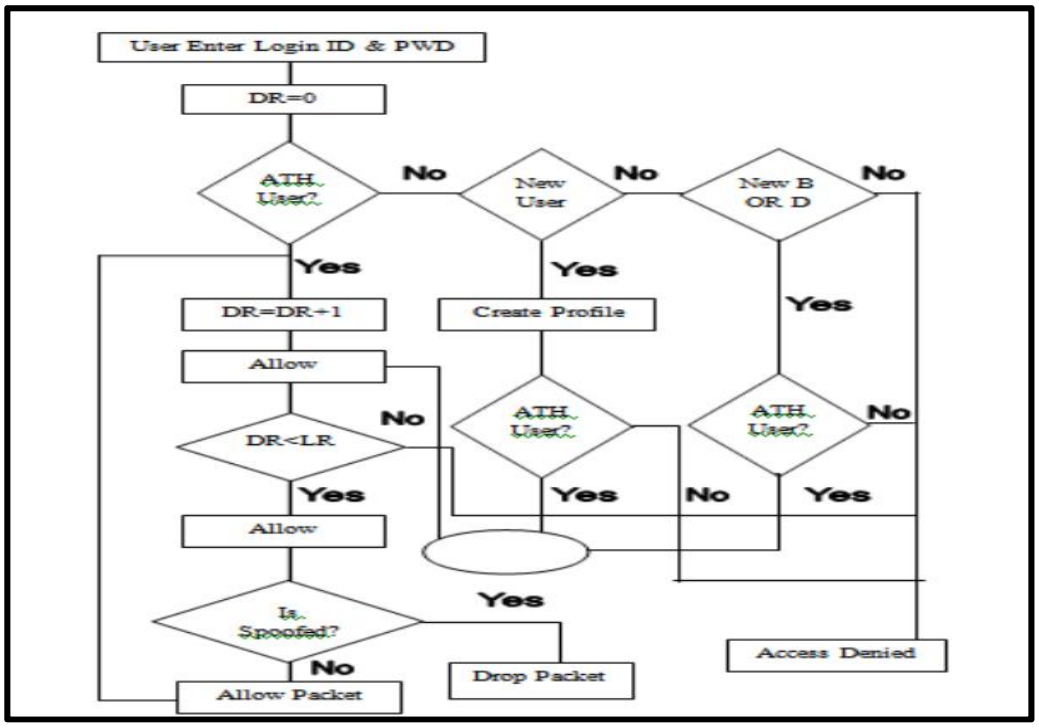

Figure 2 Flow Illustration of Planned Algorithm

UID, PWD, ATH, D, and Ball stand for User ID, Password, Authentication, User Attempt, New Device, and New Browser, respectively, utilized by the Third Party Authenticator in this Flowchart (Filter 1). [1] User-requested queries (represented by DR) and predefined table requests (represented by LR) are denoted in Filter 2 by the corresponding symbols. The Hop-Count filtering method is used to detect packet forgeries (Filter 3).

3.1. Strategic Algorithm

Limit Requested (LR) = Maximum Number of Requests Allowed

Count of User's Requests = R (s)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

For network packets, substitute "P"
An example of a forged network packet is denoted by the letter S.
Step1: First, verify login credentials using external service (if required) First, verify the user's identity.
Step 2: Compare R with LR // **2. Compare the limit of requests**
If [R>LR]
Goto step 5;
Endif
Step 3: Check the Packets using Hop-Count Method // **3. Check the spoofed packets**
If [P==S]
Discard packet;
Endif
Step 4: Repeat step 2& 3 while user logout
Step 5: Service Denied and Exit

FIRST FILTER: In the first instance, the user is authenticated by a third-party authentication service, and this continues even if the user switches between devices or browsers. A successful pass through this filter verifies that no malicious users are accessing cloud resources. Throughout the authentication procedure, each live value will be cross-referenced against a database of previous values. We're using four tables—T1, T2, T3, and T4—to keep track of things like users' login credentials and the devices and browsers they've registered with the system, as well as the phone numbers at which they signed up to receive their unique IDs.

The procedure will look like this:

First, the user inputs the ID and password, and if the profile doesn't already exist, he or she establishes a new profile by entering the mobile number registered with third-party authentication; if this is successful, the data is saved in tables T1, T2, and T3. However, if access is denied, the message "access denied contact your CSP" will be shown.

After successfully authenticating the user by entering their ID and password, the system will check to see if the user's current device and browser have been recorded in the system's history database. If they haven't, further authentication via a third party will be required before the user's information is added to T2. In any other case, the "accessdeniedcontacttoCSP" message will be shown.

Jump to the 2nd Filter algorithms

Comprehensive Procedures for Step 1 (Authentication):

Tables used

T1=Stored all information of user (whole profile)
T2=Store information of device and browser using by users
T3=Stored user ID and password
T4=Stored register mobile numbers Lists with user identification for send the One Time Password (OTP)

Variables used

LID=User ID which is entered by the user using browser
TLID=User ID which is stored in Table 3 (T3)
PWD=User password which is entered by the user using browser
TPWD=User password which is stored in Table 3 (T3)
OTP=A number generate by third party on registered mobile numbers
UOTP=A number is entered by the user at the time of creation of profile
UDev=User device which is used by the currently
UBrow=Browser which is used by the user currently
TUDev=User device history which is stored in T2
TUBrow=Browser history which is stored in T2

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

Step 1: Input login ID & Password and compare from the T3
If [LID≠TLID AND PWD≠TPWD]
Print: Does Not Exist‖
Print: Create New Profile‖;
If [UOTP≠OTP] // third party authentication
Print: Contact your Cloud Service Provider‖
Go to step 4;
Endif
If [UOTP==OTP] //third party authentication
Add record T1, T2 and T3
Go to step 3;
Endif
Endif
Step 2: Associate expedient and browser used by the user presently
If [UDev≠TUDev OR UBrow≠TBrow]
//third party authentication on registered mobile number
If [UOTP≠OTP] // third party authentication by OTP
Print: Contact your Cloud Service Provider‖
Go to step 4;
Endif
If [UOTP==OTP] //third party authentication
Add new entry in T2
Go to step 3;
Endif
Endif
Step 3: Accept requests and check if they conform to a predefined set using
Step 4: Exit

SECOND FILTER: The second filter is used to limit the user's access to optional features and tools.Since no one can intentionally or accidentally deliver more flood with this filter, everyone can rest easy. Our server will be immune to DDoS and other types of distributed denial of service attacks as a result. Here, we are keeping track of how far each user has gone toward their request limitations by utilizing table T5, and we are regularly changing the value in the "currently utilized" column. In this case, we'll assume that hourly limitations are in place for requests.
If a user exceeds a certain number of requests during a given time period, further service cannot be provided until the next session begins. If a user is allowed 200 requests per hour but exhausts that allowance in 30 minutes, he or she will not be able to use the system again until the following hour begins.
Jump to the 3rd Filter algorithms
Detailed Algorithms for Step 2 (Limit):
Table(s) used
T5= Used to store the information of requests limit and demanding requests
Variables used
LR= Predefined limit of requests //
R= Number of requests demanding by User(s)
Step 1: Count R and update Table T5 with R
Step 2: Compare R with LR
If [R>LR]
Print: Access Denied‖
Go to step 4;
Endif

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

Step 3: Allow packets and check the packets
Step 4: Exit

THIRD FILTER:

Our third filter is a variant of the Hop-Count Filtering technique. In contrast to the original suggested technique, which relied on evaluating four situations to identify valid packets, our implementation only has to consider two. When compared to the prior suggested method, this one is far more robust. This prevents any spoofing packets from being accepted.

The IP packets are filtered using Hop-Count Filter (HCF)algorithms, which require constant monitoring as they move across cloud networks in order to retrieve information such the Synchronous Flag, TTL (Time to Live), and Source IP. For each collected packet, it can identify two distinct scenarios (modified 4-cases with 2).

Synchronous Flag (SF=1) must be set in both circumstances; otherwise, the packet will be dropped without further action being taken.

If the source IP address is found in T6, the hop count is determined by utilizing the IP packet's own TTL value. If the received hop count (HS) does not match the received HC, then the source HC value in table T6 must be updated for that Source IP address (SIP).

If the source IP address is not already in table T6, then the hop count (HC) should be determined and a new entry should be made in table T6 for the TSIP (Source IP) address using the determined HC.

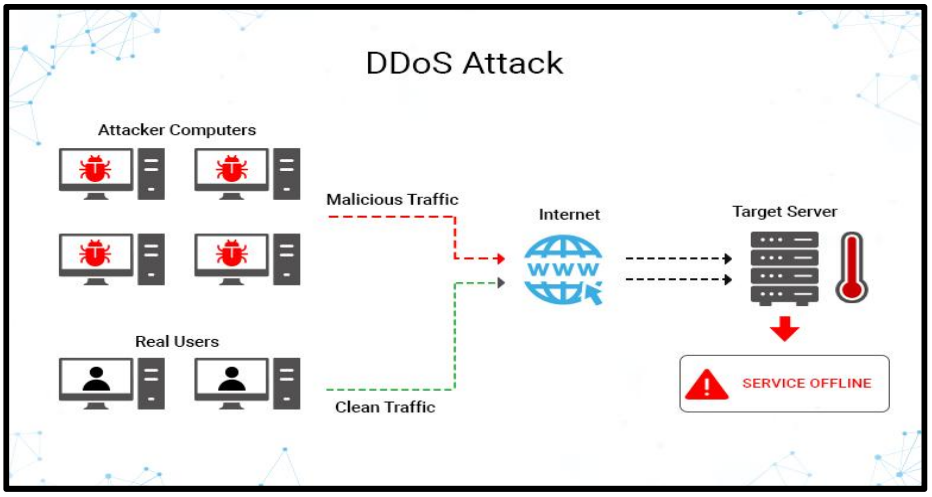

Figure 3. DDoS Attack without prevention

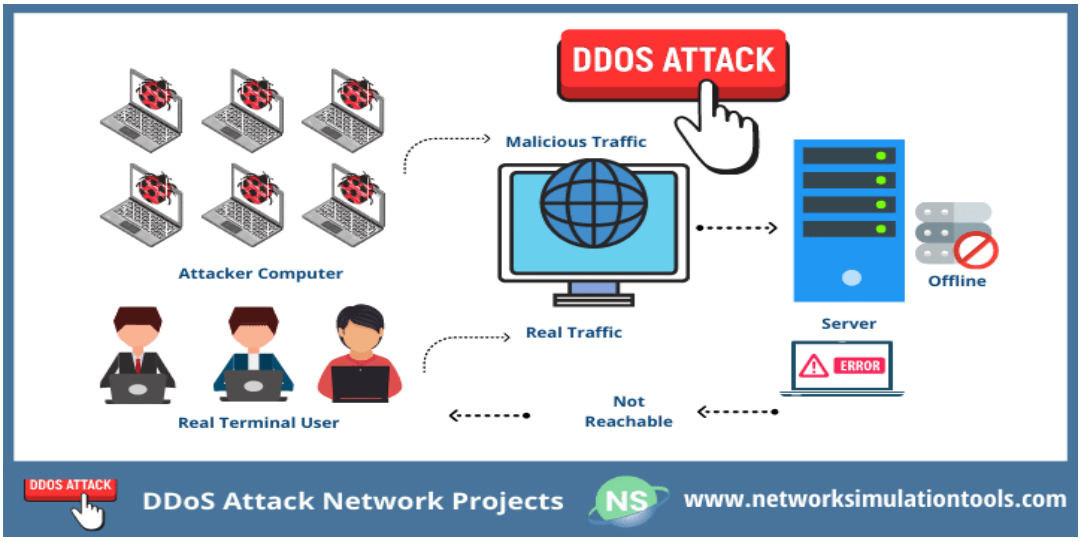

Figure 4 DDoS Attack and Prevention with proposed Algorithms

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

IV. CONSEQUENCES AND INTERPREPTION OF THE CLOUD ACCEPTANCE REVIEW

We have designed a questionnaire for primary data collection based on convenient sampling into three segments, including the IT industry, the Education Industry, and non-IT individual consumers from different organizations in order to learn more about the reasons for the limited adoption of cloud computing technology in terms of security threats. The following aims guided the development of this survey's questions.

Assessing sector-specific responses to Cloud Computing awareness. The goal of this study is to learn how different sectors feel about adopting cloud computing.

The goal of this research is to determine what is holding people back from using Cloud Computing so they can rest easy knowing that their data, networks, and websites are safe from harm.

Seven questions make up the bulk of our survey. The questions aim to measure how much worry about security is holding people back from making the switch to cloud computing. Additionally, the evaluation of industry-specific response to Cloud Computing is based on the examination of two items (out of seven questions). The next paragraphs provide an in-depth discussion, supported by graphs and SPSS software, of the statistical interpretation and analysis of the replies to seven items.

Q.1 In the IT sector, what does "Cloud Computing" basically include, and why is it important to your business?

When we posed this inquiry to the IT sector, we provided them with five potential responses.

Unsurprisingly, we observed that 60% of industrialists chose CloudComputing as A sort of outsourcing of IT, CloudComputing an intriguing technology' by 28%, CloudComputing is an unfamiliar or confusing issue' by 8% of respondents, and CloudComputing is something else for 3% of respondents.

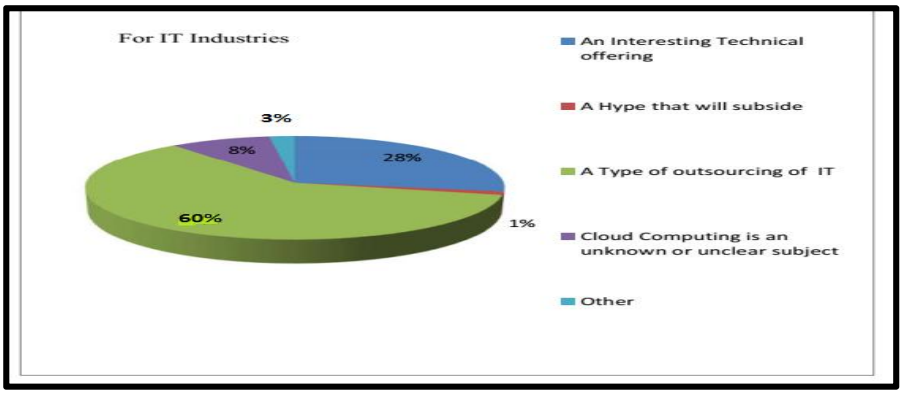

Figure 5. Cloud Computing Understanding

Question 2: What does Cloud Computing, in particular, signify for your company (the Education sector)?

We posed this inquiry to leaders and key players in the education sector, including faculty, administration, and IT personnel. We found that 43% of educators believe that "CloudComputing is an unknown or unclear subject," while 29% believe that "Cloud Computing is an interesting technical offering," 13% believe that "Cloud Computing is a hype that will subside," 11% consider "Cloud Computing a type of outsourcing of IT," and 4% believe that "Cloud Computing is something else."

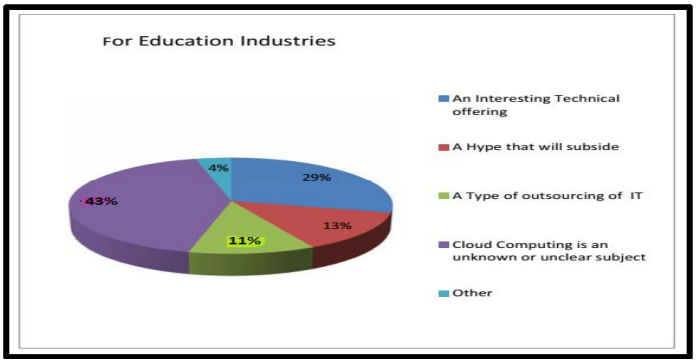

Figure 6. Cloud Computing Understanding (Education)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

Question 3: First and foremost, what does Cloud Computing represent to your business (ACROSS ALL INDUSTRIES)?

As a whole, the IT and education sectors, as well as non-IT consumers, have come to the following conclusions about cloud computing: 33% believe it to be a type of IT outsourcing, 30% believe it to be an unknown or unclear subject, 23% believe it to be an interesting technical offering, 9% believe it to be a passing fad, and 5% believe it to be something entirely different.

Therefore, the percentages are practically same between the two choices, "Cloud Computing is a kind of IT outsourcing," and "Cloud Computing is an unknown or confusing issue" for several businesses.

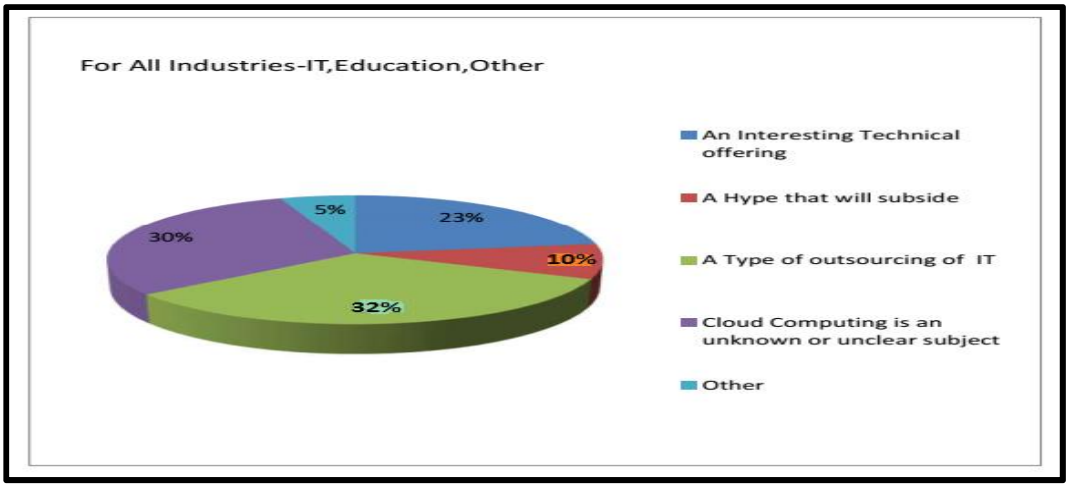

Figure 7. Cloud Computing Understanding (From All Industries) Chart

Our survey findings are also shown using a Colum Bar Chart. Data from the Colum Bar Chart demonstrates that the IT sector understands cloud computing and considers it a kind of IT outsourcing. However, the education sector and other non-IT sectors both report a lack of familiarity with cloud computing.

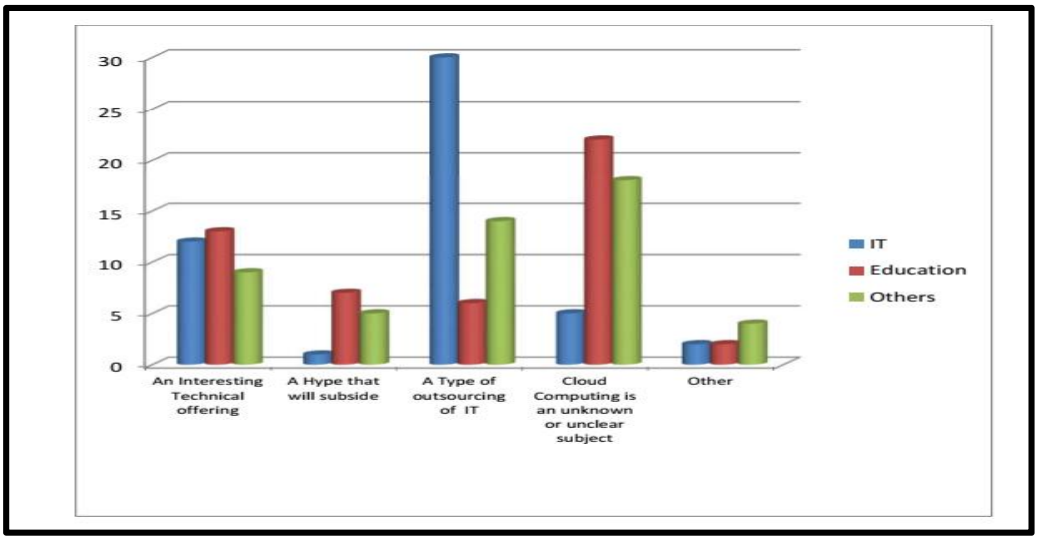

Figure 8. Cloud Computing Understanding (From All Industries)

Chart 2

Question 4: The Fourth question deals with whether or not cloud computing will be included into your company's information technology strategy. (As reported by the computer industry)?

The findings show that 37% of respondents believe Cloud Computing to be a viable option in the long term (>12 months), 31% say "Perhaps, at this moment there is insufficient knowledge within our organization to judge on utility of cloud computing," 23% believe they are already utilizing cloud computing, 2% expect to adopt cloud computing within the next 12 months, and 7% "have no intention to adopt cloud computing."

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

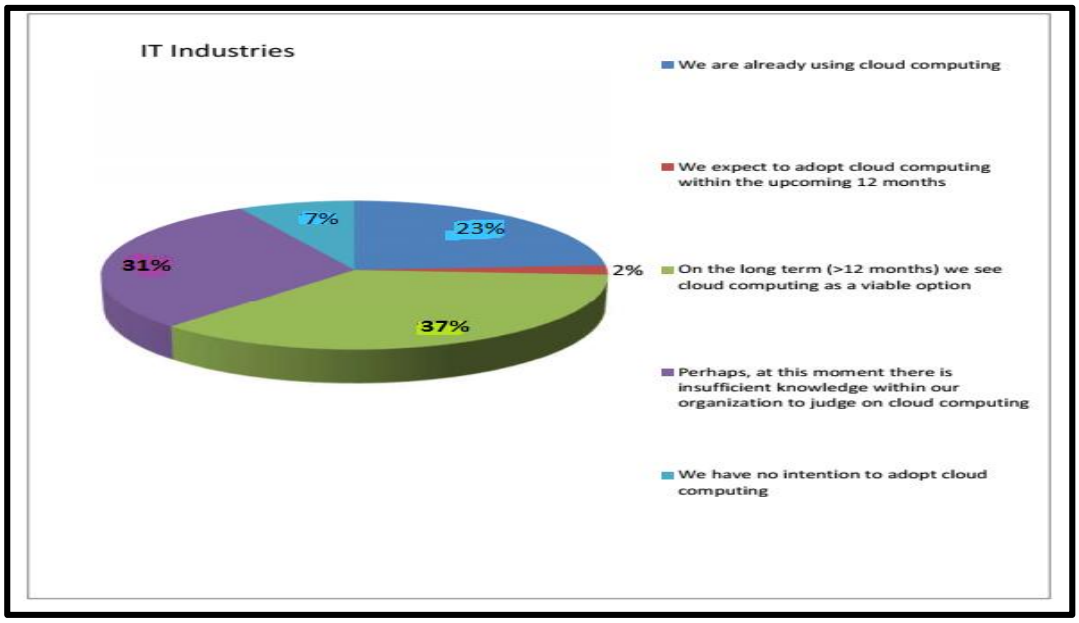

Figure 9. Acceptance of Cloud Computing (IT industries)

Question 5: The Fifth question deals with whether or not cloud computing will be included into your company's information technology strategy. (As reported by those who do not use IT)

If the chart is any indication, 37% of respondents believe that "perhaps, at this moment there is insufficient knowledge within our organisation to judge on cloud computing," 24% have no intention of adopting cloud computing, 15% say that we are already using cloud computing, 15% believe that on the long term (>12 months) they see cloud computing as a viable option, and 9% expect to adopt cloud computing within the coming 12 months.

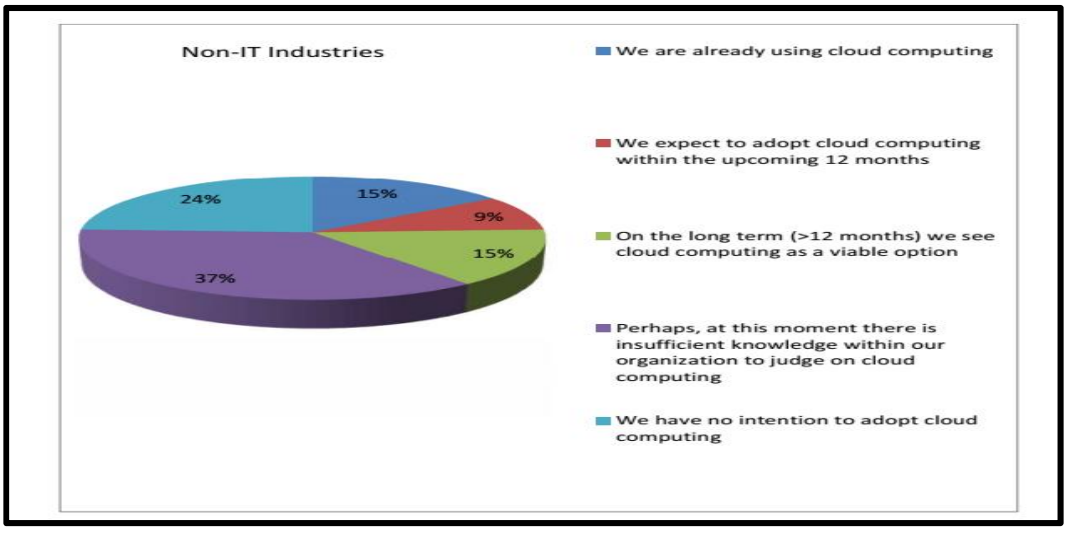

Figure 10. Acceptance of Cloud Computing (Non-IT industries)

Question 6: The second question deals with whether or not cloud computing will be included into your company's information technology strategy. (Determined by IT, Education, and Non-IT Sectors)

The data in this example has been collectively interpreted using a Pie Chart with percentages and a Column Bar Chart to show the predominant viewpoints from various sectors.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

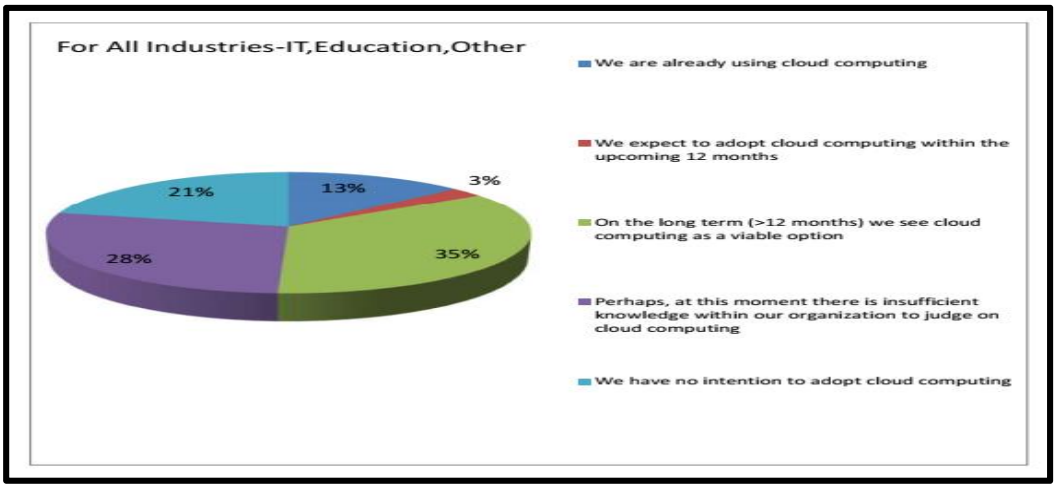

Figure 11. Acceptance of Cloud Computing (IT, Education, Non-IT)

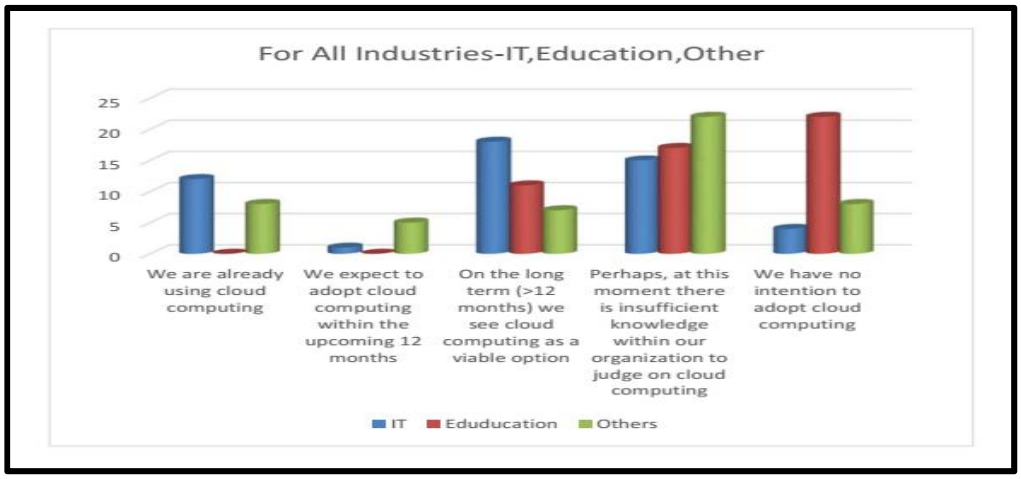

Figure 12.Acceptance of Cloud Computing (IT, Education, Non-IT)

From Figures, we can infer that 35% of respondents believe cloud computing to be a good long-term option (more than 12 months out), 28% say maybe, at this time there is insufficient knowledge within our organisation to judge the utility of cloud computing, 21% have no intention of adopting cloud computing, 13% are already using cloud computing, and 3% expect to adopt cloud computing within the upcoming 12 months. Figure 16 shows that while the IT sector sees cloud computing as a long-term (>12 months) alternative, the education sector has no plans to use it, and businesses in sectors other than IT claim they lack the necessary expertise to make an informed decision on cloud computing at this time.

Question 7 Cloud computing's potential drawbacks include fears about security breaches?

According to the replies to the question "Are security dangers a major barrier to adopting cloud computing?," it appears that this is the case. Findings reveal that 41% According to the replies to the question "Are security dangers a major barrier to adopting cloud computing?," it appears that this is the case. Findings reveal that 41%

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

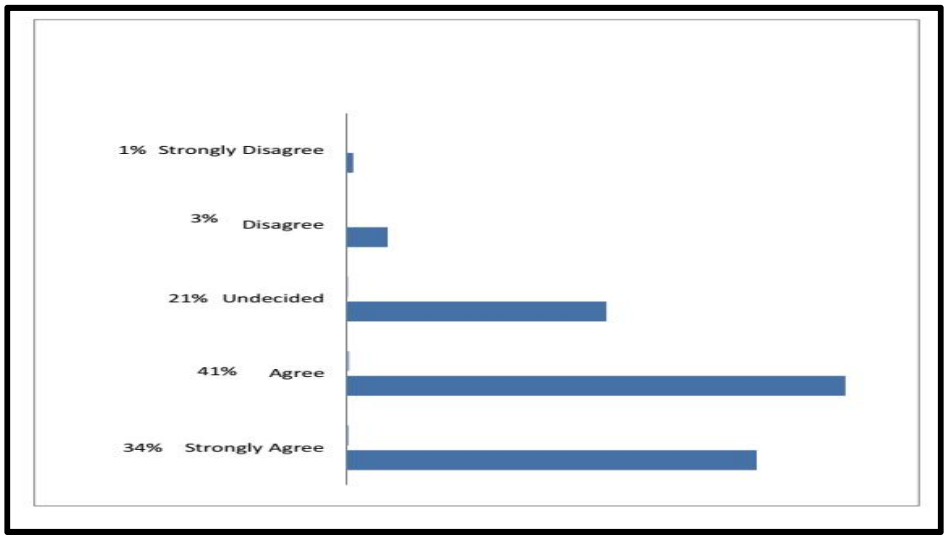

Figure 13 . Safety Extortions Concern

V. CONCLUSION

Cloud computing is widely considered as a game-changing development in recent history. Cloud computing offers scalability, rapid elasticity, measurable services, and more. One of its biggest benefits is the money it can save enterprises.

All businesses should implement cloud computing. This paper addresses a research gap in cloud computing security risks and attacks. After analyzing existing research, create algorithms as indicated solutions and implement them. For our survey, we used questionnaires. Project goals. This research aims to fill a gap in. Cloud security functions. To find the study gap and continue the investigation, more than 25 research articles were reviewed. To solve similar issues. Three research subfields are identified. Network attacks, data attacks, and reluctance are in question.

Cloud-computing implementation. Investigation yielded actionable results. Ongoing improvements to cloud computing security. Our solutions include algorithms. Explained the reasons for resistance and provided strategies to overcome them, allowing for wider adoption of cloud computing. Also discussed how future research in the same area should be conducted.

REFERENCES

[1] AnupBhange, Dr Harsh Mathur"Performance Evaluation, Analysis and Design of an Innovative Structure toSecure the Payment Gateways using Hybrid Cryptography" Asian Journal of InformationTechnology Volume: 20, Issue 2, 2021 ISSN: 1682-3915

[2] AnupBhange, "DDoS Attacks Impact on Network Traffic and its Detection Approach"International Journal of Computer Applications (0975 – 8887) Volume 40– No.11, February 2012

[3] AnupBhange, "Anomaly Detection and Prevention in Network Traffic Based on Statisticalapproach and α-Stable Model "International Journal of Advanced Research in Computer Engineering& Technology ISSN: 2278 – 1323 Volume 1, Issue 4, June 2012.

[4] AnupBhange "Comparative Analysis of Several Cryptography Algorithm with Its Effectivenesstowards the Security and Its Performance" in JGRS (UGC CARE) ISSN: 0374-8588 Volume 21Issue 6 October 2019

[5] Wayne A. Janssen, —Cloud Hooks: Security and Privacy Issues in Cloud Computing—,44th Hawaii International Conference on System Sciences, January 2011

[6] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin,IonStoica,andMateiZahria, —A view of Cloud Computing‖, Communications of the ACM, Volume 53, Issue 4, April 2010

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

[7] Mike TerLouw and Venkatakrishnan V.N. ―BluePrint: Robust Prevention of Cross-Site Scripting Attacks for Existing Browsers‖, 30th IEEE Symposium on Security and Privacy, May 2009

[8] Flavio Lombardi and Roberto di Pietro,―Secure Virtualization for Cloud Computing‖, Journal of Network and Computer Applications, Academic Press Ltd. London, UK, Volume 34, Issue 4, July 2011

[9] Chen Y, Paxson V, Katz RH (2010) What is New About Cloud Computing Security? Technical Report UCB/EECS-2010-5, University of California at Berkeley,eecs.berkeley.edu/Pubs/TechRpts/2010/EECS- 2010-5.html.

[10] Bernard Golden Different Cloud survey, Same Cloud Adoption Concern 30-9-13, http://www.enduserexperience.info/articles/share/380689/.