IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 7, July 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 7, July 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1107060 |

# Security Implications in Cloud Computing

**Rajkumar Show, Vivek Kumar**

PG Student, Dept. of CSE, IKGPTU, Swami Vivekanand Institute of Engineering & Technology, Banur, Rajpura, Punjab, India

Assistant Professor, Dept. of CSE, IKGPTU, Swami Vivekanand Institute of Engineering & Technology, Banur, Rajpura, Punjab, India

**ABSTRACT**: Cloud computing is one of the fastest-growing technologies in the IT sector. It is a concept for providing ubiquitous, practical, and on-demand network access to collections of computer resources such networking devices, servers, storage, applications, and services. Due to the various advantages the cloud has to offer, several firms have migrated their data there. However, since physical infrastructure is outsourced to a third party, cloud data storage presents a serious security risk. Using internal infrastructure, businesses may develop and maintain their own security standards, but how can they know what security measures cloud providers are doing and how well they are working? The cloud computing industry is also trying to come up with a solution for this issue. We want to create a security benchmark for cloud computing. By creating a single standard, all service providers and developers may follow the same guidelines to build a unified cloud environment, raising the bar for cloud computing security to new heights.

**KEYWORDS**: Security Implications In Cloud Computing; Rajkumar Show; Vivek Kumar; the world of cloud computing; new security standard; security lifetime; Cloud computing security; Cloud security risks; Cloud data breaches; Cloud security best practices; Cloud compliance issues; Cloud privacy concerns; Cloud encryption; Multi-tenancy security; Cloud authentication; Cloud identity and access management (IAM); Cloud service provider security; Cloud vulnerability management; Cloud audit and logging; Cloud incident response; Cloud network security; Cloud data protection; Cloud risk assessment; Cloud compliance frameworks (e.g., GDPR, HIPAA); Cloud data sovereignty; Cloud security certifications (e.g., ISO 27001, SOC 2); Zyber Software; security weaknesses;

## I. INTRODUCTION

A parallel and distributed computing system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements (SLAs) established through negotiation between the service provider and customers,' is how cloud computing is defined (Cloud Computing Definition). "When using cloud computing, the range of resources available changes based on customer demand; it grows when there is a high demand for services and shrinks when there is a low demand (Liu 2012)." But cloud computing also creates security issues since it basically takes control of the data away from the data owner.

Security is a key issue in the world of cloud computing and the cornerstone of cloud development. Due to security concerns, businesses and consumers are reluctant to fully embrace the cloud environment. Many businesses consider using cloud service providers but decide against doing so because they don't trust the security measures in place. There are several methods for data loss in the cloud to happen, despite claims by cloud computing companies that user data is safe, secure, and protected from threats. Right now, when launching a new cloud service, providers may choose to either create their own standards or follow those created by the CSA, NIST, IEEE, or ENISA. As a consequence, the industry becomes disorganised, and its parts are unable to work together. Customers' viewpoints The sheer quantity of security measures merely confuses us, and we have no idea how secure the providers are. Academics predict that cloud computing will have a huge impact on the future of the IT industry, but this development is being seriously stymied by the lack of a widely accepted standard. Therefore, developing a new security standard is essential for cloud computing development. By adhering to a single standard, we can build a fresh unified cloud environment that is more robust and better equipped to protect user data from attacks. The advantages of current technologies might be merged in a new standard to enhance the security of cloud computing. A significant finding is that combining many solutions at once might hinder the development of cloud computing in the future since no one security can effectively protect data stored in the cloud from hackers. So, adhering to a single standard could be a means to guarantee cloud computing security.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 7, July 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1107060 |

The project proposal consists of six parts. A brief review of cloud computing in general and its security requirements will be provided in the introduction of this article. The aims and objectives of the study will be covered in the second part. We also go through the Background and the Research Gap in part three. Section 4 discusses Research Innovation and Significance. Section 5 presents a few suggestions for methods based on this. The key conclusions are summarised in Section 6 along with some suggestions for further study.

## II. RESEARCH AIMS AND OBJECTIVES

**Research Aims:** To begin with, we want to make it quite obvious that the main aim of our investigation is to locate a new security standard for cloud computing. As was already said, the adoption of so many standards has made the environment for cloud computing rather chaotic, and it is now having difficulty finding out how to progress. Therefore, by upholding a single norm, this problem may be overcome. There are two reasonable justifications for why cloud computing needs a new security standard.

To begin with, because cloud computing is a relatively new system that incorporates a number of technologies, including network, storage, computers, and information technology, it requires a novel technology that is different from those currently in use. Almost all security measures in use today were developed before the cloud industry took off. "On a dedicated server, users may occupy a full system without having to share their resources with anybody else, giving them total control over the hardware, operating system, and other elements of the server." In cloud settings, the effectiveness of security measures that worked well on traditional infrastructure could not be completely realised.

Second, despite the fact that cloud computing employs a variety of security measures, the majority of cloud service providers only choose one of them to protect customer data. A single cloud computing security technique is inadequate to provide a strong defence against sophisticated cyber-attacks, according to Rong, Nguyen, and Jaatun (2012). Cloud service providers must combine several techniques into one system in order to raise the level of security in cloud computing. Combining several security measures might make up for a deficiency in one method by utilising its advantages. "As a consequence, we are able to provide a strong defence against potential attacks."

**Research Objectives:** The major aim will be achieved by pursuing three objectives: examining existing security practises, learning about a new software named Zyber, and contrasting Zyber with current security practises.

The first step is to examine some typical security methods used by cloud providers to safeguard their customers' data. This objective should provide a comprehensive overview of cloud computing security. The results will enable us to pinpoint the advantages of modern security methods and the justification for cloud providers' choice to use them while developing their systems. It may also draw attention to certain security weaknesses, enabling us to fix them and setting a new benchmark for cloud computing security.

The next objective is to concentrate on Zyber, a brand-new cloud computing application. Zyber is being developed and supported by the Canadian government. We also want to reevaluate Zyber's prospective performance by focusing on its features, including how it functions, the sort of encryption technique it uses, how much it costs to provide a better security solution than current approaches, and so on. We'll also look at its positives and negatives.

Based on the results of the first two goals, we want to compare Zyber with modern security methods. This comparison will concentrate on the advantages and disadvantages of various approaches as well as some unique aspects of Zyber. The study's main objective is to ascertain if Zyber can establish a new standard for cloud computing security.

## III. REVIEW OF LITERATURE

The current haphazard growth of cloud computing reduces its competitiveness in the IT industry and raises the danger of security breaches. According to Martinez & Pulier (2012), many firms no longer employ cloud infrastructure, despite the fact that it may have numerous advantages for enterprises, since the computing capacity provided by cloud providers lacks security, control, and administration. The three main areas of security risks that must be guarded against are data availability, confidentiality, and integrity, according to (Zissis & Lekkas 2012).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 7, July 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1107060 |

The first issue is data confidentiality. Ryan (2013) notes that since data are hosted on cloud systems, managers are more open to bribery. Managers may progressively lose their willpower when faced with conflicts of interest. Due to the fact that the cloud is a shared-tenant environment, anybody except the data owners, such as hackers or employees of third parties, may access the data stored in the cloud database. The bulk of IT infrastructure and data storage are now managed by outside vendors, according to Rong, Nguyen, and Jaatun (2012), which has two detrimental effects. First off, since cloud servers are located in faraway locations, data owners have little influence over the IT infrastructure. As a consequence, it is essential for cloud service providers to establish guidelines for their security practises in order to ensure data privacy. The second is that cloud service providers have extensive control over and unauthorised access to consumer data and applications. Customers that utilise business models with stringent security needs in particular are more likely to be continually worried about the safety of their data and have less faith in cloud providers as a result.

Previous studies have recognised the second security issue in cloud computing as the integrity risk. Gogna (2012) notes that data saved on a cloud server may change while being sent. Data loss concerns still exist even if the cloud provider's infrastructure is more reliable than that of a personal device. Rong, Nguyen, and Jaatun (2012) claim that the architecture of the provider permits the alteration of important data without user consent. Users greatly rely on the accuracy and veracity of the data, thus it must be maintained. However, there isn't a rule that may be used to regulate those cloud service providers in the cloud industry. According to Wang et al. (2010), some cloud service providers may even reclaim storage by deleting seldom used data in an effort to boost revenues.

Data accessibility is the third biggest problem with cloud computing security. Users using cloud services are unable to access their data in the event of a server or hard drive failure since they have no access to the system directly. According to (Rao & Selvamani 2015), cloud providers are very concerned about availability since data is scattered among servers in remote locations. If the cloud server goes down, more users will suffer than in the traditional arrangement (Rong, Nguyen & Jaatun 2012).

As was previously said, switching to a cloud environment could have certain drawbacks, but other research have provided a number of strategies to lessen these issues. First off, CSA (2013) and Rong, Nguyen, and Jaatun encourage cloud computing customers to use a better encryption (2012). This would prevent data from being sent in plain text to cloud service providers and other unauthorised users prior to being received by the authorised users (Rong, Nguyen & Jaatun 2012). Further, Sun at et al. (2014) suggest that cloud storage should be built on the dependability of hard drives, calling for greater infrastructure research. Choo (2010) argues that cloud service providers need to build their storage facilities throughout a number of urban areas.

In several reviews of current research, many alternative solutions have been proposed to decrease the negative consequences of the move to cloud computing. They all work really hard to provide the best degree of data security in cloud computing. "However, none of them realised that what was necessary was to build a new cloud environment by developing a new model that everyone could use." At the moment, it is also a research gap.

## V. RESEARCH SIGNIFICANCE

The current haphazard growth of cloud computing reduces its competitiveness in the IT industry and raises the danger of security breaches. According to Martinez & Pulier (2012), many organisations no longer employ cloud infrastructure, despite the fact that it might have numerous advantages for enterprises, since the computing capacity provided by cloud providers lacks security, control, and administration. The three main areas of security risks that must be guarded against are data availability, confidentiality, and integrity, according to (Zissis & Lekkas 2012).

The first issue is data confidentiality. Ryan (2013) notes that since data are hosted on cloud systems, managers are more open to bribery. "Managers may progressively lose their willpower when faced with conflicts of interest." Due to the fact that the cloud is a shared-tenant environment, anybody except the data owners, such as hackers or employees of third parties, may access the data stored in the cloud database. The bulk of IT infrastructure and data storage are now managed by outside vendors, according to Rong, Nguyen, and Jaatun (2012), which has two detrimental effects. First off, since cloud servers are located in faraway locations, data owners have little influence over the IT infrastructure. As a consequence, it is essential for cloud service providers to establish guidelines for their security practises in order to ensure data privacy. The second is that cloud service providers have extensive control over and unauthorised access to

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 7, July 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1107060 |

consumer data and applications. Customers that utilise business models with stringent security needs in particular are more likely to be continually worried about the safety of their data and have less faith in cloud providers as a result.

Previous studies have recognised the second security issue in cloud computing as the integrity risk. Gogna (2012) notes that data saved on a cloud server may change while being sent. Data loss concerns still exist even if the cloud provider's infrastructure is more reliable than that of a personal device. Rong, Nguyen, and Jaatun (2012) claim that the architecture of the provider permits the alteration of important data without user consent. Users greatly rely on the accuracy and veracity of the data, thus it must be maintained. However, there isn't a rule that may be used to regulate those cloud service providers in the cloud industry. According to Wang et al. (2010), some cloud service providers may even reclaim storage by deleting seldom used data in an effort to boost revenues.

Data accessibility is the third biggest problem with cloud computing security. Users using cloud services are unable to access their data in the event of a server or hard drive failure since they have no access to the system directly. According to (Rao & Selvamani 2015), cloud providers are very concerned about availability since data is scattered among servers in remote locations. If the cloud server goes down, more users will suffer than in the traditional arrangement (Rong, Nguyen & Jaatun 2012).

As was previously said, switching to a cloud environment could have certain drawbacks, but other research have provided a number of strategies to lessen these issues. First off, CSA (2013) and Rong, Nguyen, and Jaatun encourage cloud computing customers to use a better encryption (2012). This would prevent data from being sent in plain text to cloud service providers and other unauthorised users prior to being received by the authorised users (Rong, Nguyen & Jaatun 2012). Further, Sun at et al. (2014) suggest that cloud storage should be built on the dependability of hard drives, calling for greater infrastructure research. Choo (2010) argues that cloud service providers need to build their storage facilities throughout a number of urban areas.

In several reviews of current research, many alternative solutions have been proposed to decrease the negative consequences of the move to cloud computing. They all work really hard to provide the best degree of data security in cloud computing. However, none of them realised that what was necessary was to build a new cloud environment by developing a new model that everyone could use. At the moment, it is also a research gap.

Several hundred IT experts, many of whom are now engaged in cloud-related initiatives, participated in the joint IEEE/CSA poll. 93 percent of survey participants said they believed cloud computing security standards were necessary, and 82 percent said they felt this requirement was urgent (ProQuest n.d.). Furthermore, 44 percent of respondents indicated they are actively involved in defining cloud computing standards, while 81 percent of respondents said they were likely or somewhat likely to do so in the next 12 months (ProQuest n.d.).

Director of IEEE-managing SA Judy Gorman states. 'The Cloud Security Alliance and IEEE are the natural partners to set the baseline on the demands, attitudes, and behaviours around cloud security standards as well as the existing and prospective utilisation of cloud computing services. The Cloud Security Alliance is the top worldwide organisation for cloud security, and IEEE is a world authority on developing standards for a dizzying array of sectors. The survey's results will be useful in directing the future growth of the cloud community.' The Cloud Security Alliance recommends a list of 10 steps that customers of cloud services should take to evaluate and manage the security of their cloud environments in order to reduce risk and provide the appropriate level of support. n.d. (ProQuest). These ten stages are being developed, albeit they have not yet been standardised. The final official criteria will be comparable in comparison. Organizations who want to use the cloud in their operations and follow tried-and-true guidelines that have been assessed by all relevant authorities and experts in cloud security should take these 10 measures into consideration.

Steps include:

- Step 1: Verify the existence of efficient governance, risk, and compliance processes

- Step 2: Audit operational and business processes

- Step 3: Manage people, roles, and identities

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 7, July 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1107060 |

- Step 4: Ensure adequate data and information protection

- Step 5: Enforce privacy rules.

- Steps 6: through 9 involve assessing security provisions for cloud applications, checking the safety of cloud networks and connections, evaluating security measures for physical infrastructure and facilities, and managing security terms in cloud service level agreements.

- Step 10: Recognize the exit procedure's security requirements.

## VI. RESEARCH METHODOLOGIES

Warfield (2010) asserts that utilising a combination of quantitative and qualitative research methods as opposed to a single research methodology improves the validity of the findings. The highlighted study goal and proposed objectives are met using a variety of research techniques, including quantitative and qualitative methods. "More specifically, quantitative techniques are used for online survey methods, whereas qualitative approaches are chosen for interview, evaluation research, and comparison research."

Each strategy is closely tied to our study goals and aim since it was selected for a certain stage of the research.

In order to direct our own study, we modified Cao et al. (2006)'s framework, which consists of four primary acts, to match our research. Among these reshaped activities are theory formulation, observation, assessment, and justification. First, the phase's guiding principle. This stage should result in data points and numbers that have also undergone analysis. "Therefore, one of the essential methods is doing online surveys." Online polls and discussion boards could be a part of this. Research questions are important because they specify the subjects that a study wishes to look at, according to Timothy & Levy (2009). Furthermore, surveys collecting quantitative data should be created in a confirmatory and predictive way, claim Timothy & Levy (2009). As a consequence, some of our fictitious questions about cloud computing may be:

Question 1 - Discussion board - How secure is end-to-end encryption when transmitting data? (Confirmatory)

Question 2 - Users in General - How will cloud computing affect your career, study, and social life if security is significantly improved? ( Predictive)

It is important to remember that over the course of the investigation, a potential issue with data validity will need to be addressed. In conclusion, the outcomes of this stage are essential for conceptually advancing our research objective.

Observations make up phase two. If a study question requires a more in-depth examination of a specific social phenomenon at this point, the case studies technique is highly suggested. As a result, case studies and literature reviews are employed as supporting tools in our research to conduct a comparative analysis. A literature review's foundation is reviews of a variety of academic publications. "The primary focus is on current security issues and their solutions." The results of this phase are essential in assisting the subsequent stage since case studies are conducted with the goal of finding solutions. According to Wynn & Williams (2012), a case study should focus on actions occurring inside a specific framework, such a single business. In order to evaluate existing solutions and compare their advantages and disadvantages in light of certain organisational events, we will conduct case studies. Overall, the creation of hypotheses that will be tested during the experimental step is aided greatly by this stage.

The next phase is evaluation and justification. According to Cao et al. (2006), a variety of conventional approaches, such as interviews, may be used to conduct system assessments. Furthermore, according to Cao et al. (2006), understanding an IT artefact completely requires merging system evaluation and theory testing operations. "As a consequence, we released an evaluation study on Zyber, a still-in-development technology, for both theoretical testing and interviews." Previous studies have shown Zyber to have significantly improved cloud computing security, and this is also the basic tenet of our study approach. After its first release or during beta, Zyber will first undergo testing.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 7, July 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1107060 |

The usefulness of Zyber will be assessed based on its performance, usability, consistency, availability, reliability, and degree of security. We will also conduct interviews with possible targets like the CEO and development team of Zyber. As a result, our suggested hypothesis may be supported by the evaluation's results.

A success assessment approach must be employed in respect to the three main goals we stated after each research phase. Data analysis is done after analysing phase results and before comparing with stated goals. It's also vital to remember that the research approaches you've selected are not phase-exclusive and necessary, which means you might, depending on the circumstance, utilise a range of tactics or more flexible choices.

## VII. CONCLUSION

In conclusion, cloud computing is becoming more widely accepted, and many companies are switching to cloud-based infrastructure since it is a modern and developing trend in technology. However, security flaws continue to pose a severe hazard to users of cloud services. The three key issues that function as barriers to cloud adoption are, in order, data availability, data integrity, and confidentiality. The main study objective is to find a new standard that is safe enough for businesses and individual users to adopt. For us to succeed, a number of objectives must be accomplished. These objectives include evaluating existing solutions, testing new technologies, and comparing them. The significance of the study's results must be emphasised since they have the potential to completely transform cloud computing. More customers could benefit from cloud computing's advantages. "Furthermore, data from previous investigations provide strong support for our suggested hypothesis." In addition to online surveys, literature reviews, case studies, interviews, and a more general strategy that focuses on assessing Zyber technology, our research team has selected a variety of significant research approaches. Ultimately, by following a broad framework and set of guidelines, as well as by including principles in the research process and using modern research technology, significant and accurate research findings are predicted.

## REFERENCES

1. Choo, R.K. 2010, Cloud computing: Challenges and future directions, Australian Institute of Criminology, Canberra, viewed 8 September 2015, <http://aic.gov.au/publications/current%20series/tandi/381-400/tandi400.html>
2. Gogna, M. 2013, ‘A survey on security challenges of Cloud Computing’, International Journal of Computer Science & Communication, vol. 4, no. 1, pp. 21-23.
3. Grance, T. & Mell, P. 2011, Recommendations of the National Institute of Standards and Technology, 800-145, National Institute of Standards and Technology (NIST) Special Publication 800-145, U.S. Department of Commerce, the United State.
4. Martinez F. R. & Pulier E. 2012, ‘System and method for a cloud computing abstraction layer with security zone facilities’, U.S. Patent Application Publication, no. 13/354,275.
5. Rao, R.V. & Selvamani, K. 2015, ‘Data Security Challenges and Its Solutions in Cloud Computing’, Procedia Computer Science, vol 48, pp. 204-209.
6. Robert, K.Y. 2013, Case Study Research: Design and methods, 5th edn, Sage publications, London.
7. Rong, C., Nguyen, S.T. & Jaatun, M.G 2012, ‘Beyond lightning: A survey on security challenges in cloud computing’, Computers and Electrical Engineering, vol. 39, no. 1, pp. 47-54.
8. Ryan M.D. 2013, 'Cloud computing security: The scientific challenge, and a survey of solutions' , Journal of Systems and Software, vol. 86, no. 9, pp. 2263-2268.
9. Timothy, J.E & Levy, Y. 2009, ‘Towards a Guide for Novice Researchers on Research Methodology: Review and Proposed Methods’, Issues in Informing Science & Information Technology, vol. 6, pp. 323.
10. Top Threats Working Group 2013, The Notorious Nine Cloud Computing Top Threats in 2013, Cloud Security Alliance (CSA).
11. Wang C, Chow, S. S. M. , Wang Q, Ren K, Lou W. 2010, 'Privacy-preserving public auditing for data storage security in cloud computing//INFOCOM' , Proceedings IEEE, San Diego, CA, pp. 1-9.
12. Warfield, D. 2010, ‘Information Systems (IS) and Information Technology (IT) research: A research methodologies review’, Journal of Theoretical & Applied Information Technology, vol. 13, pp. 28-25.
13. Wynn, J.D. & Williams, C.K. 2012, ‘Principle for conducting critical realist case study research in information system’, MIS Quarterly, vol. 36, pp. 787.
14. Zissis, D. & Lekkas, D. 2010, ‘Addressing cloud computing security issues’, Future Generation Computer Systems, vol. 28, no. 3, pp. 583-592.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details