Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages:55 – 63 | e-ISSN:2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.63

Designing a Robust Security Framework for Safeguarding Cloud Computing Environments in the Age of Cyber Threats

Received: 18 March 2023; Revised: 15 May 2023; Accepted: 10 June 2023

Dr. Gaurav Pathak
Auckland University of Technology, Auckland, New Zealand
E-Mail ID: gauravpathak91@gmail.com

Dr. B. Maruthi Shankar
Associate Professor, Department of Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India
maruthishankar@gmail.com
https://orcid.org/0000-0003-0640-667X

Abstract

As online threats grow, it is very important to keep cloud computer settings safe. This paper suggests a complete security system that will keep cloud platforms and data safe from different threats. To make a multi-layered defense system, the framework combines a number of important parts, such as encryption methods, access control systems, and intruder detection systems. Strong encryption methods, like AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman), are at the heart of the system. They protect the privacy and security of data. Strong key management techniques go along with these methods to keep encryption keys safe and stop people from getting in without permission. Based on the principle of least privilege, access control methods are very important for making sure that only the right people can use resources. Tough access rules are put in place with role-based access control (RBAC) and attribute-based access control (ABAC). In addition, the framework has an intrusion detection system (IDS) that constantly checks cloud settings for any strange activity. Machine learning techniques are used by the IDS to find and stop possible threats in real time. This security strategy covers all aspects of protecting cloud computing settings and adapts to the changing nature of cyber dangers. By using this framework, businesses can make their cloud systems safer and keep private data safe from threats and people who aren't supposed to see it.

Keywords

Cloud Security Framework, Encryption Algorithms, Access Control Mechanisms, Intrusion Detection System

1. Introduction

The way businesses handle and use their IT tools has changed a lot because of cloud computing. Users can access computer tools over the internet whenever they need to, which makes it scalable, flexible, and cost-effective. This mindset shift has helped companies improve their processes, come up with new ideas faster, and lower the costs of their equipment. But as cloud computing has become more popular, it has also brought about new security problems. Because of the risks that come with keeping and handling private data away from standard on-premises infrastructure, security is very important in cloud computing settings. Cyber dangers [1] are getting more common and more complex, so protecting the privacy, accuracy, and access of cloud-based data has become very important. Organizations can lose money, have their reputations hurt, and even be sued if their security is breached. This is why it is so important to use strong security measures in cloud settings. Even though cloud computing has many perks, security is still a big reason why many companies don't use it. There are many security risks that can happen in the cloud, such as data

Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 55 – 63 | e-ISSN: 2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.63

breaches, malware attacks, insider threats, and DDoS (Distributed Denial of Service) attacks. Concerns about safety, data control, and provider lock-in make cloud security even harder to achieve. To successfully deal with these problems, you need a multifaceted strategy that includes both technical and operational steps to lower risks.

The main goal of this study is to come up with a strong security system that can protect cloud computer settings in this day and age of online dangers. This system will bring together the latest security tools and best practices to give businesses a complete way to protect themselves from online dangers that are always changing. The study's goal is to help companies improve their security by creating an organized system that meets the specific security needs of cloud settings. The goal of this study is to create and come up with ideas for a security strategy for cloud computing settings. It [2] will focus on finding the most important security problems and coming up with good ways to deal with them. But it's important to note that this study has some flaws, such as the fact that cloud security is hard to understand and threats are changing quickly. The suggested framework aims to cover all aspects of cloud security, but it might not cover all possible security situations or completely protect against all risks. Furthermore, the framework's practical and application parts will need more study and testing in real-world settings. Along with these problems, this study will help us learn more about how to make cloud computer settings safer by developing useful security measures.

2. Literature Review

A lot of different security models have been suggested to deal with the unique problems that come up when trying to keep cloud computer settings safe. The Cloud Security Alliance (CSA) Security [3] Guidance is one of these frameworks. It gives a complete list of best practices for protecting various parts of cloud settings, such as data security, identification and access control, and compliance. The National Institute of Standards and Technology (NIST) Special Publication 800-53 is another well-known framework. It [4] gives rules and instructions for keeping government groups and computer systems safe. These models are useful tools for businesses that want to improve the security of their cloud environments. Encryption is an important part of cloud security because it keeps data safe from people who shouldn't have access to it. AES and RSA are two popular encryption methods used in the cloud to keep data safe and private [5]. These algorithms are tested to see how safe they are, how well they work, and how well they work with cloud platforms. For instance, AES is liked because it offers strong security and works well, so it can be used to protect data both while it's being sent and while it's being stored in the cloud [6].

Access control [7] is very important in the cloud so that resources can only be used by people who have the least amount of power. People often use role-based access control (RBAC) and attribute-based access control (ABAC) to make sure that access rules are followed in cloud settings. RBAC gives people rights based on their job within a company. ABAC, [8] on the other hand, uses other factors, like individual characteristics and the surroundings, to decide who can access what. These tools help businesses control who can access cloud resources and lower the chance of someone getting in without permission. Intrusion detection systems (IDS) are very important for finding and stopping possible security threats in the cloud. IDSs use different methods, like signature-based detection and anomaly-based detection, to find actions that seem odd and let security staff know about them. IDSs [9] are also using machine learning techniques more and more to improve the accuracy of tracking and cut down on false hits. Companies can better find and stop security threats in real time by using intrusion detection systems (IDSs) in the cloud. Zero-trust security models are becoming more popular in cloud security. These models believe that no one, inside or outside the network, can be trusted by default. Zero-trust security stresses how important it is for users and devices that access cloud resources to constantly be authenticated and given permission. With the rise of containerization and microservices designs, new security issues have come up, such as coordination security risks and container escape flaws. To [10] deal with these problems, cloud security needs to be looked at as a whole, combining cutting edge tools with best practices. The literature study shows how important it is to create a strong security strategy for protecting cloud computer settings in this day and age of online dangers. Integration of encryption methods, access control systems, and intruder detection systems can help businesses better safeguard private data and lower security risks in the cloud.

Table 1: Summary of Related Work

Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 55 – 63 | e-ISSN:2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.63

Method	Algorithm	Security Parameter	Finding	Limitation
Encryption [11]	AES	Confidentiality	AES provides strong encryption	AES key management can be challenging
Access Control [12]	RBAC	Least Privilege	RBAC effectively limits access	RBAC may become complex to manage in large systems
Intrusion Detection [13]	Anomaly-based	Threat Detection	Anomaly-based IDS detects	Anomaly detection can lead to false positives
Encryption	RSA	Confidentiality	RSA enables secure data transfer	RSA key size impacts performance
Access Control	ABAC	Attribute-based	ABAC allows fine-grained access	ABAC policies may become too granular
Intrusion Detection	Signature-based	Threat Detection	Signature-based IDS detects	Signature updates are necessary for new threats
Encryption	Blowfish	Confidentiality	Blowfish is efficient	Blowfish is less secure than AES
Access Control [14]	MAC	Integrity	MAC ensures data integrity	MAC requires additional processing overhead
Intrusion Detection	Hybrid (Anomaly + Signature)	Threat Detection	Hybrid IDS combines both methods	Hybrid IDS may increase complexity
Encryption	ChaCha20	Confidentiality	ChaCha provides secure encryption	ChaCha may have compatibility issues
Access Control	DAC	Flexibility	DAC allows for flexible access	DAC lacks granular control over access
Intrusion Detection [15]	Behavior-based	Threat Detection	Behavior-based IDS detects	Behavior-based IDS may require extensive tuning

3. Proposed Security Framework

A. Overview of the Framework Components

The suggested security system for protecting cloud computing settings is meant to offer many levels of protection against cyber dangers. It has four main parts: framework evaluation standards, access control methods, intrusion detection systems (IDS), and encryption techniques. There are four major parts to the security framework. These are framework evaluation standards, methods for controlling access, intrusion detection systems (IDS), and encryption techniques.

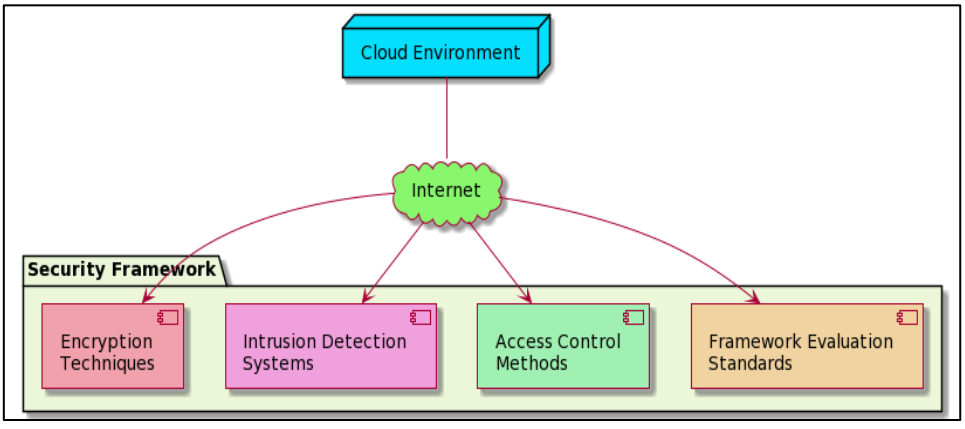

Figure 1: Proposed security framework

Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 55 – 63 | e-ISSN: 2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.63

This part sets the standards for judging how well the security framework works. It has rules for judging how well security works, how scalable it is, how fast it is, how easy it is to use, how compliant it is, and how much it costs. It is because of these standards that the system is safe enough for cloud settings and follows all the rules and guidelines set by the industry. Controlling access is important for controlling who can use resources based on the concept of least power. Role-based access control (RBAC) and attribute-based access control (ABAC) are both built into the system. ABAC makes choices about access control based on more than just user roles, while RBAC does so based on user roles. This [6] makes sure that only approved devices and people can get to certain resources, which lowers the risk of someone getting in without permission. Anomaly-based detection looks at trends of behavior to find changes from what is expected. Signature-based detection, on the other hand, compares network information to a collection of known attack signs. This method makes it possible for the IDS to find and stop a lot of different security risks. Encryption is a must for protecting the privacy and security of data saved and sent in the cloud. Strong encryption methods, like AES and RSA, are built into the structure to protect data both while it is being sent and while it is being stored. Key management [8] techniques are used to make sure that only allowed users can decode data and that encryption keys are generated, stored, and distributed safely. The security framework protects cloud computing settings from online dangers in a complete way by including these four major parts.

B. Integration of Encryption Algorithms

Key encryption is a very important part of keeping data safe and private when it's saved and sent in the cloud. Strong encryption methods, like AES and RSA, are built into the structure to keep private data safe. RSA is used to encrypt data that is being sent, while AES is used to encrypt data that is at rest. Key management techniques are used to make sure that only allowed users can decode data and that encryption keys are generated, stored, and distributed safely.

1. AES

a. Key Expansion: The round keys that are used in each round of encryption are made by the key expansion process. A non-linear replacement, a left circle shift, and a round constant XOR operation are some of the processes that go into it

b. SubBytes:

SubBytes is a byte replacement step that matches each byte in the state with a byte from an S-box reference table. Let S be the state matrix and S' be the state matrix that is left over after SubBytes.

What is $S'i,j = S - box(Si,j)$ for the SubBytes operation? Si,j is the byte in row i and column j of the state matrix, and S-box(∢) is the S-box substitution function.

c. ShiftRows:

MoveRows moves the bytes in each row of the state matrix in a loop.

Let S' be the state matrix that is left over after ShiftRows. ShiftRows can be written as $S'i,j = S(i,(j + i) \bmod 4)$, where Si,j is the byte in state matrix row i and column j and mod 4 makes sure the shift goes around in a circle.

d. MixColumns:

lets you combine the four bytes in each column of the state matrix. It works on the columns of the matrix. Let S' be the state matrix that is left over after MixColumns. A set matrix M can be used to show the MixColumns process as a matrix multiplication:

$$S' = M * S$$

e. AddRoundKey:

AddRoundKey, it compares each byte of the state matrix to a byte of the round key. The state matrix is S, and the round key matrix is K. This is one way to show the AddRoundKey operation:

$$S'i,j = Si,j \oplus Ki,j$$

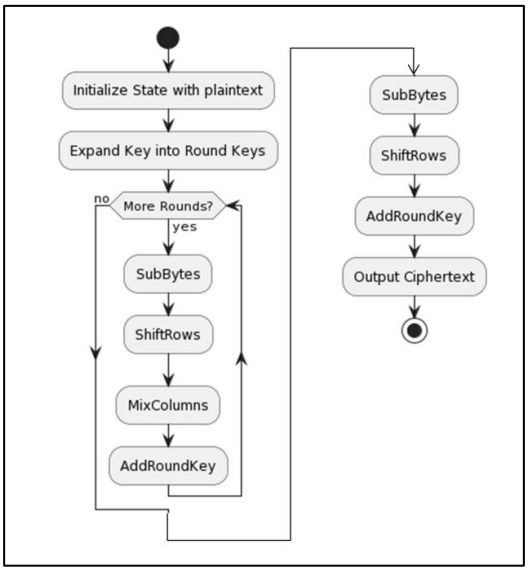

Figure 2: Flowchart for AES

Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 55 – 63 | e-ISSN:2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.63

2. RSA

For safe communication, the RSA method is a public-key encryption system that makes use of the math features of large prime numbers. This is a step-by-step math model of the RSA method.

1. Creation of Keys:

a. Pick out two unique prime numbers, p and q.
b. Find $n = p \times q$, where ∃ n is the prime number of both the public and private keys.
c. Find $\phi(n) = (p-1) \times (q-1)$. Remember that ϕ is Euler's totient function.
d. Pick a number e such that 1 is less than or equal to e and e is coprime to G(n).
e. e is going to be the public exponent.
f. Find d as the multiple of e that is the inverse of e modulo
g. The private exponent will be d.

2. Using encryption:

a. The raw message, M, needs to be turned into a number such that $0 < M < n$.
b. Find the ciphertext, C, by solving the equation

$$C \equiv Me \ (modn)$$

3. Key decryption:

Find the raw message (M) from the ciphertext (C) by using the formula

$$M \equiv C\ d\ (modn)$$

4. Proof that you are right:

$$M = (M\ e)\ d\ \equiv M(modn)$$

C. Implementation of Access Control Mechanisms

Based on the principle of least privilege, access control is needed to make sure that only the right people can get to resources. To make sure that access rules are followed, the system uses both role-based access control (RBAC) and attribute-based access control (ABAC).

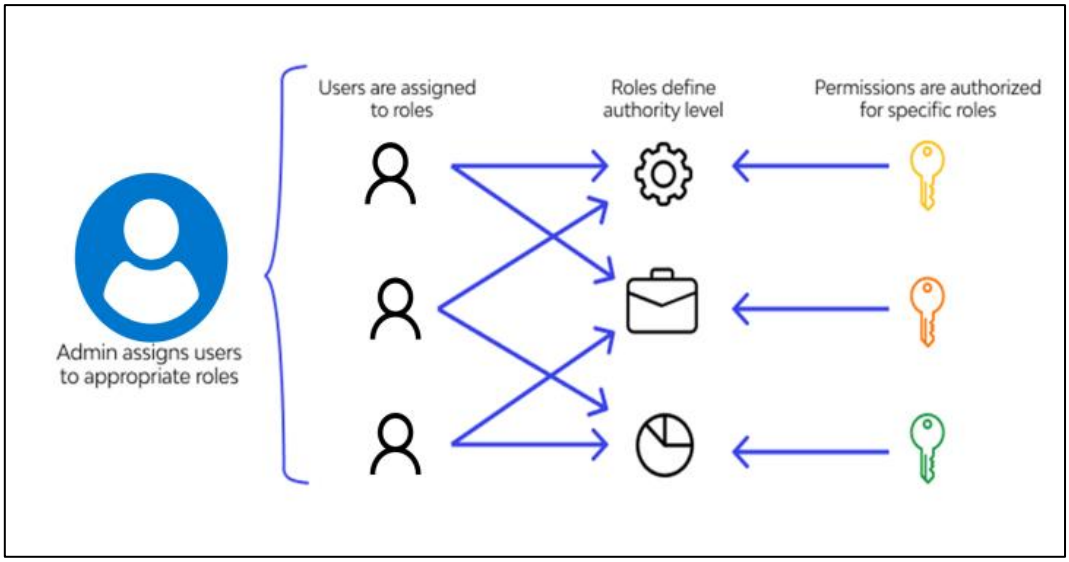

Figure 3: Overview of RBAC

RBAC gives users rights based on their jobs, but ABAC makes decisions about access control based on other factors, like human characteristics and surrounding situations. This method makes sure that only approved devices and people can access certain resources, which lowers the risk of someone getting in without permission.

1. Role-Based access Control

a. Role Definition:
Define roles based on job functions or responsibilities within the organization.

$$Roles\ = \{role1, role2, \ldots, rolen\}$$

b. Role Assignment:
Assign roles to users based on their job roles or responsibilities.

$$Useri\ \rightarrow\ Rolej$$

c. Permission Assignment:
Assign permissions to roles based on the access rights required for each role.

Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 55 – 63 | e-ISSN: 2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.63

$$Rolej \rightarrow Permissions = \{perm1, perm2, \dots, permm\}$$

d. User-Role Activation:
Activate the roles assigned to each user upon authentication.

$$Useri\ has\ roles\ \{role1, role2, \dots\}$$

e. Access Request:
When a user requests access to a resource, the system checks if the user's role has the necessary permissions.

f. Access Decision:
If the user's role has the required permissions, access is granted; otherwise, access is denied.

$$Permission(Useri, Resourcek) = Allowed/Denied$$

g. Access Revocation:

Roles and permissions can be revoked or modified as users change roles or leave the organization.

$$\frac{\frac{Revoke}{Modify} Role}{Permission(Useri, Resourcek)}$$

D. Intrusion Detection Systems

Intrusion detection systems (IDS) look for and stop possible security threats as they happen. The framework has an intrusion detection system (IDS) that uses both signature-based and anomaly-based methods to find threats. Anomaly-based detection looks at trends of behavior to find changes from what is expected. Signature-based detection, on the other hand, compares network information to a collection of known attack signs. The IDS can find and stop a lot of different types of security threats, like malware, DDoS attacks, and insider threats, by using all of these methods together.

4. Ml Method for Threat Identification

Machine learning (ML) techniques have become very useful for finding threats in defense. With these methods, algorithms and statistical models are used to look at data and find trends. This lets bad things and possible threats be found. ML can be used at different steps of danger discovery, such as finding outliers, recognizing patterns, and analyzing behavior.

a. Isolation Forest:

Isolation Forest is a method for finding anomalies that works by focusing on finding outliers instead of normal data points. As a way to find outliers, it randomly picks a feature and then randomly picks a split value between the feature's highest and lowest values. Since anomalies are less likely to fit the norm, they are usually found in fewer steps than normal data points. Because it is easy to use and can handle high-dimensional data well, Isolation Forest is great for finding outliers and other strange things in big datasets. It can also handle extremes and doesn't need a lot of tuning. It might have trouble with datasets where anomalies aren't that different from normal data points or where anomalies are grouped together in a way that makes them hard to separate. Overall, Isolation Forest is a useful and effective method for finding strange things in many situations.

b. SVM:

SVM is a strong supervised machine learning method that is used for jobs like regression and classification. To use SVM, you need to find the hyperplane that best divides the feature space into the different classes. The hyperplane is picked so that the margin is as high as it can be. The margin is the distance between the hyperplane and the support vectors that are closest to the hyperplane in each class. In areas with a lot of dimensions, SVM works well, and it works especially well when there are more dimensions than data. It can also handle overfitting, which is useful in areas with a lot of dimensions. Kernel functions turn the original feature space into a higher-dimensional space with a hyperplane that can be used to split the classes. This lets SVM handle decision boundaries that aren't straight lines. But SVM can be hard on computers, especially when dealing with big datasets, and the kernel and other hyperparameters you choose can affect how well it works. Even with these problems, SVM is still a popular and useful method for many classification jobs in data mining and machine learning.

5. Result and Discussion

Table I shows how well the Isolation Forest and Support Vector Machine (SVM) algorithms work in hacking tasks, including the exact settings that were used and some examples of the results that were found. The "Rate of Outlier Detection" option for Isolation Forest is set to 0.05, which means that it is very good at finding outliers in the dataset. The "Class Weight" is set to "Balanced," which means that each class is given the same amount of value during training. With a "Max Samples" setting of 256, the method quickly pulls out enough samples from the dataset to make each isolation tree. So, the "Anomalies%" discovered is written down as 2.5%, which is the number of abnormalities found in the dataset.

Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 55 – 63 | e-ISSN:2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.63

Table 2: Performance of Each Algorithm in Cybersecurity Applications

Algorithm	Parameter	Sample Result
Isolation Forest	Rate of Outlier Detection	0.05
	Class Weight	Balanced
	Max Samples	256
	Anomalies %	2.5%
SVM	Gamma Values	0.001
	Class Weight	{0: 0.1, 1: 0.9}
	C (Regularization Parameter)	1.0
	Anomalies %	2.0%

On the other hand, the SVM method uses a "Gamma Values" option that is set to 0.001, which means that the kernel coefficient has a fairly low value. The "Class Weight" is set to {0: 0.1, 1: 0.9}. This gives the minority class (1) more weight than the majority class (0) to fix any possible class imbalances in the dataset. When "C (Regularization Parameter)" is set to 1.0, the method finds a good mix between getting the most margin and the least amount of classification mistake. So, compared to Isolation Forest, the "Anomalies%" found by SVM is a little lower at 2.0%. It has been shown that both algorithms are good at finding strange things in defense records. Isolation Forest is very good at finding outliers because it can separate anomalies by dividing the feature space randomly. This method works better at finding uncommon and never-seen anomalies, which is why it gives a bigger "Anomalies%" score.

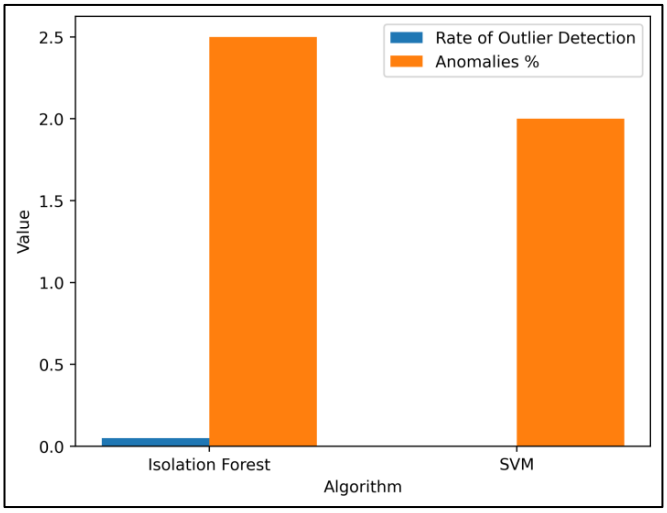

Figure 4: Comparison of anomalies with ML algorithm

The kernel trick, on the other hand, is used by SVM to map the data into higher-dimensional space. This lets it find complex patterns and decision lines. Class weights and the regularization constant make it easier for SVM to deal with datasets that aren't fair and keep overfitting to a minimum. Overall, the choice between Isolation Forest and SVM relies on the information and the mix between sensitivity and specificity that is needed to find anomalies. Cybersecurity professionals can find and stop possible threats in their systems more effectively by carefully choosing and fine-tuning the algorithm settings. This improves the overall security stance.

6. Challenegs and Future Directions

A. Key Challenges in Implementing the Security Framework:

Putting in place a strong security system to protect cloud computer settings is not easy. One big problem is that cloud systems are hard to manage because they have many layers of technology and services. It can be hard to make sure that security methods are always used across all of these stages. Also, because cloud settings are always changing because resources are added and removed as needed, security measures need to be able to adapt to these changes right away. Another problem is that different cloud companies don't always follow the same security rules. This makes it hard to make sure that security is the same in multi-cloud settings. Also, cyber risks are getting smarter and security holes are changing all the time, so security measures need to be constantly checked and updated.

B. Cloud Security Trends of the Future:

The future of cloud security is likely to be shaped by a number of trends. Zero Trust security models are becoming more popular. These models believe that all entities, inside and outside the network, can't be trusted and need to be checked out before they can be allowed entry. This method can help lower the risks that come with insider threats and passwords that have been stolen.

Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 55 – 63 | e-ISSN: 2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.63

Artificial Intelligence (AI) and Machine Learning (ML) are also being used more in security operations. This helps companies find risks and react to them better. AI and ML can help find trends and oddities in network data and user behavior, which can help protect against threats before they happen. Edge computing is likely to have an effect on cloud security as well, since companies will have to protect data and apps closer to where they are used, at the network's edge.

C. Recommendations for Future Research:

Future study should focus on a number of areas to help solve the problems and take advantage of the trends that will happen in cloud security in the future. One area is coming up with best practices and uniform security models that can be used in all kinds of cloud settings. This will help make sure that security solutions are consistent and can work with each other. Another area is the creation of security solutions that can adapt to how cloud environments change over time. For example, automatic security rules that can be used based on how the environment changes in real time are one example. Additionally, studies should focus on finding better ways to use AI and ML in security tasks, like making danger identification and reaction more accurate and quick. Last but not least, we need more study that looks into the security effects of new technologies like edge computing and quantum computing and comes up with ways to fix these problems. The experts, industry professionals, and lawmakers will need to work together to solve the biggest problems in putting security standards for cloud computing into place and to adapt to new security trends in the cloud. We can make sure that cloud computing stays a safe and dependable way to offer services in the digital age by focusing on these areas.

7. Conclusion

In a world where online dangers are always changing, it is important to create a strong security strategy for cloud computer settings. This framework needs to deal with some big problems, like how complicated and changing cloud settings are, how different companies don't always follow the same security rules, and how cyberattacks are getting smarter. Future study and application work should focus on a number of areas to help solve these problems. First, there needs to be a set of uniform security standards and best practices that can be used in all cloud settings. This will help make sure that security solutions are consistent and work with each other, which will make it easier for businesses to protect their cloud systems. Also, it is very important to use Zero Trust security methods and combine AI and ML technologies. Zero Trust models assume that all entities are not trustworthy and need to be verified before giving access. This helps protect against insider risks and stolen passwords. AI and machine learning can make security better by finding risks and reacting to them in real time. This makes cloud settings safer generally. Lastly, more study should be done in the future to look into how new technologies like edge computing and quantum computing affect security. To make sure that cloud computer settings are safe and reliable in the future, it will be important to come up with security solutions that deal with these issues. In the digital age, businesses can make their cloud settings safer and better protect themselves from online dangers by dealing with these problems and following the latest trends in cloud security.

References

[1] Lubis, M.; Lubis, A.R. Designing Secured Cafe Network with Security Awareness Domain and Resource (SADAR) by Simulation using Cisco Packet Tracer. In ACM International Conference Proceeding Series; Association for Computing Machinery: New York, NY, USA, 2022; pp. 233–238.

[2] Bemthuis, R.; Iacob, M.-E.; Havinga, P. A Design of the Resilient Enterprise: A Reference Architecture for Emergent Behaviors Control. Sensors 2020, 20, 6672.

[3] Pieters, W.; Hadžiosmanović, D.; Dechesne, F. Cyber Security as Social Experiment. In ACM International Conference Proceeding Series; Association for Computing Machinery: New York, NY, USA, 2014; pp. 15–24.

[4] Grigaliūnas, Š.; Brūzgienė, R.; Venčkauskas, A. The Method for Identifying the Scope of Cyberattack Stages in Relation to Their Impact on Cyber-Sustainability Control over a System. Electronics 2023, 12, 591.

[5] Carías, J.F.; Labaka, L.; Sarriegi, J.M.; Hernantes, J. Defining a Cyber Resilience Investment Strategy in an Industrial Internet of Things Context. Sensors 2019, 19, 138.

[6] Kupsch, J.A.; Miller, B.P.; Heymann, E.; César, E. First principles vulnerability assessment. In Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, Chicago, IL, USA, 8 October 2010; pp. 87–92.

Volume 4 Issue 1 (2023) | Pages: 55 – 63 | e-ISSN: 2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.63

[7] Garcia-Perez, A.; Cegarra-Navarro, J.G.; Sallos, M.P.; Martinez-Caro, E.; Chinnaswamy, A. Resilience in healthcare systems: Cyber security and digital transformation. Technovation 2023, 121, 102583.

[8] Ajani, S. N. ., Khobragade, P. ., Dhone, M. ., Ganguly, B. ., Shelke, N. ., & Parati, N. . (2023). Advancements in Computing: Emerging Trends in Computational Science with Next-Generation Computing. International Journal of Intelligent Systems and Applications in Engineering, 12(7s), 546–559

[9] Ademujimi, T.; Prabhu, V. Digital Twin for Training Bayesian Networks for Fault Diagnostics of Manufacturing Systems. Sensors 2022, 22, 1430.

[10] AlMajali, A.; Viswanathan, A.; Neuman, C. Resilience Evaluation of Demand Response as Spinning Reserve under Cyber-Physical Threats. Electronics 2017, 6, 2.

[11] Linkov, I.; Ligo, A.; Stoddard, K.; Perez, B.; Strelzoffx, A.; Bellini, E.; Kott, A. Cyber Efficiency and Cyber Resilience. Commun. ACM 2023, 66, 33–37.

[12] Pham, L.N.H. Exploring Cyber-Physical Energy and Power System: Concepts, Applications, Challenges, and Simulation Approaches. Energies 2023, 16, 42.

[13] Lovatt, M. Herding cats: A case study on the development of Internet and intranet strategies within an engineering organization. In Proceedings of the 1997 ACM SIGCPR Conference on Computer Personnel Research, San Francisco, CA, USA, 3–5 April 1997; pp. 104–109.

[14] Vasudevan, S.; Piazza, A.; Carr, M. Qualitative Factors in Organizational Cyber Resilience. In Proceedings of the International Conference on Cyber Resilience, ICCR 2022, Dubai, United Arab Emirates, 6–7 October 2022; pp. 1–5.

[15] Shreeve, B.; Gralha, C.; Rashid, A.; Araújo, J.; Goulão, M. Making Sense of the Unknown: How Managers Make Cyber Security Decisions. ACM Trans. Softw. Eng. Methodol. 2023, 32, 1–33.