Vol. 06, No. 4 (2024) 1837-1848, doi: 10.24874/PES.SI.25.03b.016

Proceedings on Engineering Sciences

www.pesjournal.net

A CASE STUDY ON USING THREAT MODELING TO SECURE CLOUD COMPUTING DATA

N. Praneetha
S. Srinivasa Rao[1]
P. S. Brahmanandam

Received 15.11.2023.
Received in revised form 17.12.2023.
Accepted 24.01.2024.
UDC – 004.056

Keywords:

Cloud computing, Privacy or Security, Cloud Service Providers, Encryption Methods

ABSTRACT

Cloud computing (CC) is an easy way to access computer resources, which many businesses increasingly use to outsource their data. Nonetheless, privacy and security are significant concerns in CC when sharing and storing data in a distributed setting. Potential dangers to cloud data security would cause significant disruptions. This paper discusses security challenges and feasible encryption approaches. The workings of a few encryption schemes are also discussed. By identifying and mitigating potential threats, it is possible to reduce the risk of a data breach. In this connection, a case study based on threat model simulations is presented. The CC's future is bright and hopeful, albeit a few loose ends exist. Building an integrated security architecture that can regulate all cloud layers is an immediate requirement for providing highly safe cloud services. A few recommendations to protect cloud data are provided and CC's future research directions are also emphasized.

1. INTRODUCTION

Cloud computing has revolutionized the way businesses and individuals store and access data. Without cloud computing, the modern computing landscape would not be as it is today. Cloud computing development has been aided by the research works of many significant researchers. For instance, one of the earliest and most influential researchers of cloud computing was Joseph Redmon, who developed the MapReduce platform in 2004. MapReduce is a distributed computing platform that allows users to process large datasets in parallel on an array of computers. Redmon's work laid the foundation for the development of cloud computing, as his platform enabled the distributed storage and processing of large datasets on a massive scale.

Another significant researcher was James Hamilton, who developed the concept of distributed cloud computing in the late 2000s. Hamilton's work focused on the development of virtual machines and the implementation of elastic cloud computing, which allowed businesses to scale their computing resources more efficiently. Hamilton's contributions were instrumental in the development of cloud computing as we know it today. The development of cloud computing has also been aided by significant research from Amitabh Srivastava, Alexey Andreyevich, and Robert Marcus. These researchers have developed new techniques for cloud storage, distributed computing, and cloud security. Their works have enabled businesses to store and process data securely in the cloud and have helped to make cloud computing more efficient and reliable.

[1] Corresponding authors: S. Srinivasa Rao
E-mail: srinu1479cse@kluniversity.in

Apart from cloud computing, the other well-known computing paradigms are cluster computing (proposed by Gene Amdahl of IBM in 1962) and grid computing (proposed by Ion Foster and Carl Kesselman in 1999), respectively. Grid computing: A distributed computing paradigm that enables transparent resource sharing among geographically dispersed resources, typically connected through high-speed networks. This allows for on-demand access to computational power, storage, and other resources, regardless of their physical location. Cluster computing: A tightly coupled set of interconnected computers working together as a single computing resource. They typically share the same operating system, storage, and network connection, and are used for parallel processing tasks requiring high performance. Figure 1 illustrates the Google search trends pertaining to cloud computing, grid computing, and cluster computing spanning from January 2004 to January 2023. The trends delineate the relative levels of interest and inquiry manifested by users on the Google platform regarding these distinct computing paradigms over the specified time frame. This graph makes it evident that cloud computing has taken over the market since July 2007, proving that both big and small businesses as well as the general public have accepted it. It is to be noted from this figure that a value of 100 (50) is the peak popularity (half as popular) for the term, while a score of 0 means there was not enough data for this term.

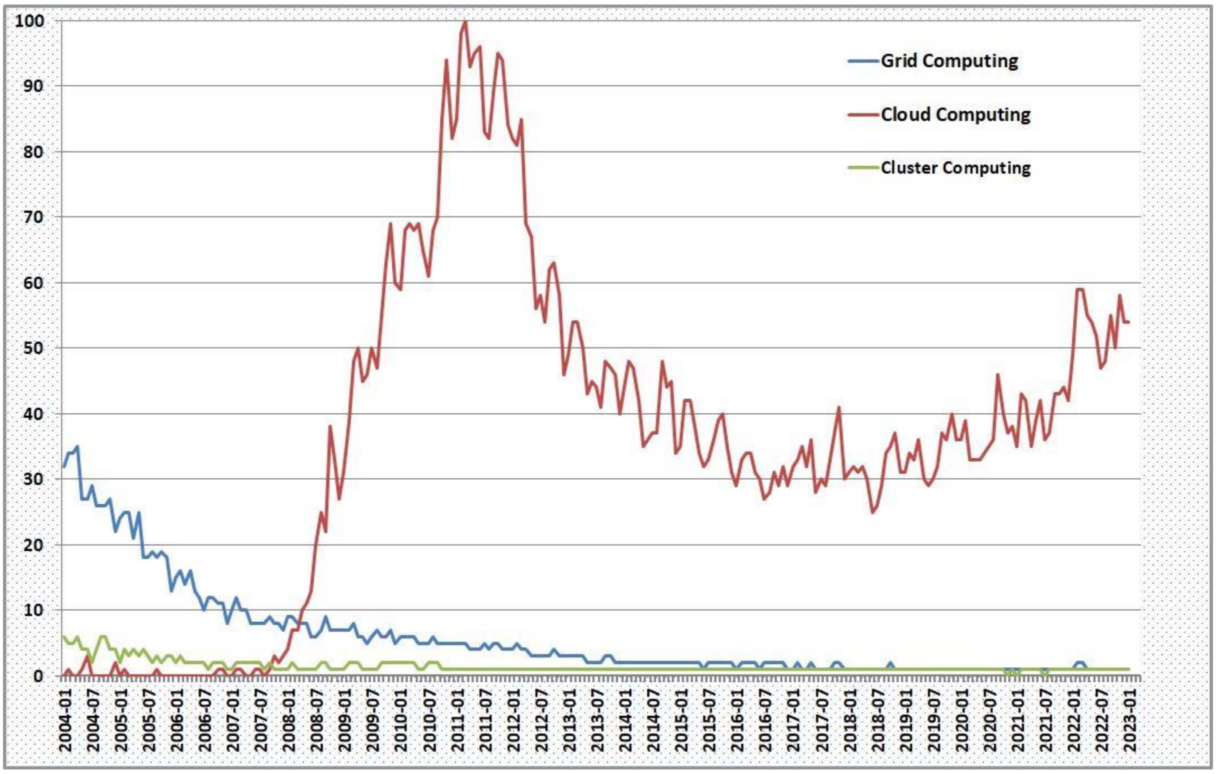


Figure 1. The popularity of Cloud Computing against Grid and Cluster Computing paradigms, according to Google Trends, from January 2004 to January 2023

Coming to the cloud computing applications, the list is so wide, which include healthcare sector (Yang et al., 2021), education sector (Kushagra & Dhingra, 2022; Alharbi et al., 2020) and agriculture (Hori et al., 2020) to name a few. It was reported that cloud computing can lower the start-up costs for electronic health records, including software, hardware, networking, staff, and license fees (Ramu & Reddy, 2015). Any evolving technology must add immense benefits to the organizations and their stakeholders, so that the adaptability of that technology will, surely, be welcomed. The healthcare industry has widely adopted cloud computing framework because it provides a number of advantages, including increased access, speed and customization of services, quick decision-making processes, optimization of costs associated with infrastructure, and simple scalability (Gao et al., 2018). The adoption of cloud computing in educational sectors has gained momentum, particularly, during the COVID-19 pandemic (Bhardwaj et al., 2020). This is because the global lockdown during the COVID-19 pandemic times forced us to administer the concept of online teaching (Agarwal & Kaushik, 2020).

There are a good number of studies that reported on the parameters that influence as well as hinder the adoption of cloud computing in the educational sector. It was stressed that the future of the education system could be restructured with the help of computer-based technology or information communication technology because it is a comprehensive approach to innovate education systems, methods, and management (Tantatsanawong et al., 2011). Alsufyani et al. (2015) underscored the significance of cloud computing within the educational domain, highlighting its capacity to diminish infrastructure setup and maintenance expenses while enhancing operational efficiency. Moreover, the authors corroborated the assertion that the adaptability and dependability inherent in cloud computing render it particularly suitable for educational settings.

The factors that motive an individual organization to shift to cloud computing and the changing significance of decisive factors, if the change is inevitable, have been discussed by (Golightly et al. 2022). The adoption of CC technology has benefited healthcare, higher education, and further education, according to the same researchers who covered these topics in-depth. The adoption of CC during and after the COVID-19 pandemic (Brahmanandam et al., 2020) has altered stakeholders' perceptions to the point where CC has demonstrated a strong ability to facilitate teaching and learning activities and may be used as a productive tool for knowledge sharing globally (Al-Hajri et al., 2021).

1.1 The Role of Encryption Methods in Cloud Computing

Cloud computing security is becoming increasingly important as businesses rely heavily on cloud-based services. Unfortunately, security threats in the cloud are numerous and constantly evolving, making it difficult to protect data and keep up with the latest cyber threats (Khan & Tuteja, 2015). Without encryption, cloud computing would not be nearly as secure or reliable as it is today. Encryption helps to protect data stored on the cloud from unwanted access or tampering, and it also helps to ensure that sensitive data is not leaked or shared without authorization.

In addition, encryption makes it possible for cloud service providers to store data from multiple users on the same servers without the risk of one user being able to access or manipulate another user's data. Encryption also ensures that data is securely transferred between the cloud and the user, so that it is not intercepted by third parties. Overall, encryption is essential for ensuring the security and reliability of cloud computing, and it provides an extra layer of protection that helps to keep data safe and secure in the cloud.

Encryption serves as a crucial mechanism for thwarting both accidental and intentional alterations to sensitive data. It is widely acknowledged that numerous institutions, governmental regulations, and industry standards mandate explicit encryption protocols. This is primarily due to the fact that robust encryption serves as compelling evidence of comprehensive data protection, devoid of vulnerabilities. During data transmission between disparate systems, various threats to data integrity and confidentiality, such as man-in-the-middle (MitM) attacks, pose significant risks (Sowah et al., 2019). The implementation of data encryption during transit, commonly facilitated by the Transport Layer Security (TLS) protocol as advocated by Dierks and Allen (1999), effectively mitigates many of these risks, ensuring heightened security measures.

Storing data in the public cloud exposes it to a broader spectrum of risks, encompassing inadvertent exposure to the internet, unauthorized access by other cloud tenants, and potential breaches by malevolent insiders within the cloud provider's infrastructure. Default encryption of data in cloud storage serves as a fundamental safeguard against these multifarious threats. With the exponential surge in remote work, characterized by the widespread storage of data beyond physical office premises and the prevalent use of personal devices to access corporate systems, ensuring universal data encryption significantly bolsters security measures in such scenarios. Intellectual property stands as a pivotal asset for numerous organizations, often bearing substantial financial value. Through the encryption of sensitive data and the meticulous management of encryption keys, organizations can effectively neutralize its utility to potential attackers, thereby safeguarding their strategic interests.

It has been stressed by many researchers that by *implementing the right security measures* and understanding the *latest cloud security threats*, businesses can ensure the security of their cloud-based systems. In those circumstances, it is imperative to understand the existing and the ensuing security threats on cloud data (both transit and rest) and feasible solutions offered by various Tech Giants. In this context, we have brought this review to provide various potential threats posed to the cloud data.

This paper is arranged as follows: In section 1, some potential mechanisms for the prevention of attacks are elaborated and it also provided the modus operandi of those potential mechanisms. In section 2, In addition, the Microsoft threat model (THREAD) is simulated to know the possible security and privacy threats. The other aim of this study is to identify some of the future research directions in this ever-growing area.

2. VARIOUS CLOUD SECURITY AND PRIVACY ATTACKS

Security considerations in cloud computing are contingent upon various factors, including the cloud service provider, cloud user, service user, and specific instance. Additionally, the security landscape is influenced by the delivery model, comprising Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (Hashizume et al., 2013). Four primary deployment methods exist: public cloud, private cloud, hybrid cloud, and community cloud, each presenting distinct security and privacy challenges.

The Cloud Security Alliance (CSA), a non-profit organization, plays a pivotal role in establishing standards, best practices, and certifications to ensure a secure cloud computing environment. According to CSA's publication "Top Threats to Cloud Computing: The Pandemic 11," released on June 7, 2022, the following threats are identified in order of priority:

i. Insufficient identity, credential, access, and key management
ii. Insecure interfaces and Application Programming Interfaces (APIs)
iii. Misconfiguration and inadequate change control
iv. Lack of cloud security architecture and strategy
v. Insecure software development
vi. Insecure third-party resources
vii. System vulnerabilities
viii. Accidental cloud data disclosure
ix. Misconfiguration and exploitation of serverless and container workloads
x. Organized crime/hackers/Advanced Persistent Threat (APT), and
xi. Cloud storage data exfiltration

We, however, briefly discuss some of the significant attacks and challenges faced by cloud computing data and their feasible solutions. The possible attacks on cloud security are presented in the following graphic. Figure 2 shows six important cloud security issues (shown in the inner box) that pose a significant threat to the cloud data and also shows the feasible solutions (shown in the outer box) that one can rely on to protect cloud data in safe mode.

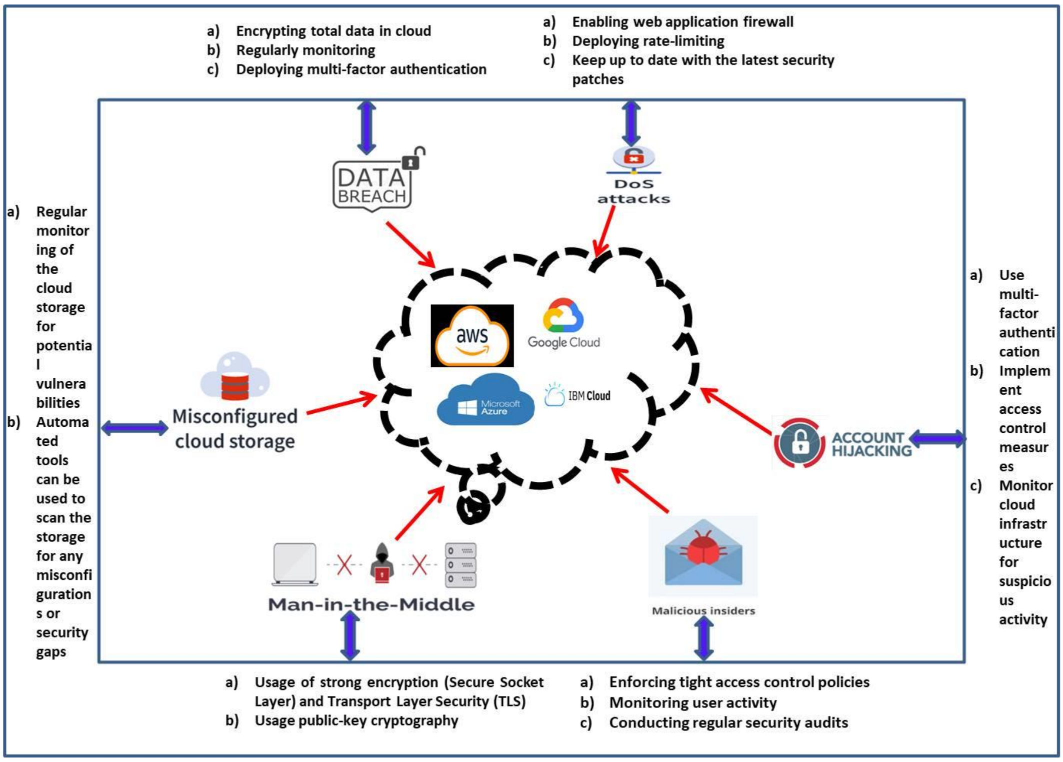

a) Encrypting total data in cloud
b) Regularly monitoring
c) Deploying multi-factor authentication
a) Enabling web application firewall
b) Deploying rate-limiting
c) Keep up to date with the latest security patches
DATA BREACH
DoS attacks
aws
Google Cloud
Microsoft Azure
IBM Cloud
a) Regular monitoring of the cloud storage for potential vulnerabilities
b) Automated tools can be used to scan the storage for any misconfigurations or security gaps
Misconfigured cloud storage
a) Use multi-factor authentication
b) Implement access control measures
c) Monitor cloud infrastructure for suspicious activity
ACCOUNT HIJACKING
Man-in-the-Middle
Malicious insiders
a) Usage of strong encryption (Secure Socket Layer) and Transport Layer Security (TLS)
b) Usage public-key cryptography
a) Enforcing tight access control policies
b) Monitoring user activity
c) Conducting regular security audits

Figure 2. Shows a few significant security threats to the cloud data, as shown in the inner box, while their feasible solutions are presented in the outer box

Cloud data security is a top priority for businesses and organizations that use cloud computing. There are numerous potential threats to cloud data security, ranging from malicious actors to human negligence. There are numerous high-profile examples of cloud data security breaches, highlighting the importance of safeguarding data stored in the cloud. The following lines provide some statistics regarding the number of security attacks on AWS, GCP, and Microsoft Azure cloud data providers.

Figure 3 shows the number of attacks on different cloud computing providers from 04 February 2018 to 31 January 2023 (almost five years). It can be seen that AWS and Microsoft Azure has shown almost equal trends, albeit a few minute differences do exist here and there. It is also estimated that every week AWS cloud provider has to face 68, the Microsoft Azure cloud provider is 48, and while GCP cloud provider receives 6 attacks, respectively. According to one survey, hackers frequently succeed in targeting smaller businesses because these establishments might be underprepared to defend themselves. Data breaches at small businesses worldwide surged by 152% in 2020 and 2021 respectively compared to 2018 and 2019.

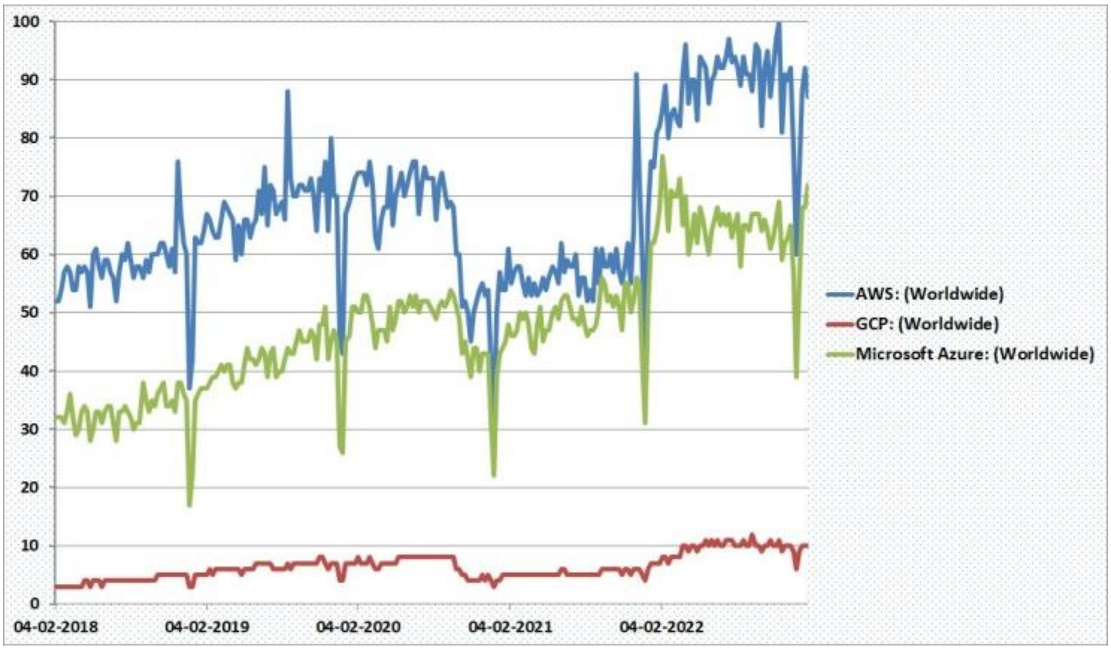


Figure 3. Number of security attacks on cloud data (AWS, Google Cloud Provider (GCP), and MS Azure) according to 'Google Trends', from 04 February 2018 to 31 January 2023 (Accessed on 31 January 2023)

Cloud computing is a rapidly developing technology that has seen a tremendous growth in usage over the past decade. According to a Forbes study, the COVID-19 rise has further fueled the establishment of the value and flexibility of cloud computing, which has led to quicker CC adoption. This growth has been accompanied by a range of security concerns, as the unique environment of the cloud introduces new challenges and vulnerabilities to traditional security measures. To protect against these threats and attacks, various security approaches have been proposed by individuals, ranging from different encryption methods and access control mechanisms to intrusion detection systems.

3. TYPES OF ENCRYPTION METHODS

In data encryption, *the transformation of data into unreadable will be done* with the aid of mathematical functions and algorithms. The encryption process makes it difficult or impossible for unauthorized users to access sensitive information. Figure 4 depicts the encryption and decryption processes in a simple manner. The cipher (a simple mathematical function/algorithm) does act as a heart for the encryption ecosystem. To elaborate, in a typical encryption method, plain text and key are combined which are, again, kept in a cipher to form a ciphertext (for example, see the flow of black arrows). Opposite to the encryption process, one can clearly understand the decryption process from the following graphic (see the flow of blue arrows). In the decryption method, a key and cipher text will be added to the cipher to transform into a plain text. Therefore, plain text will be retrieved at the receiving end.

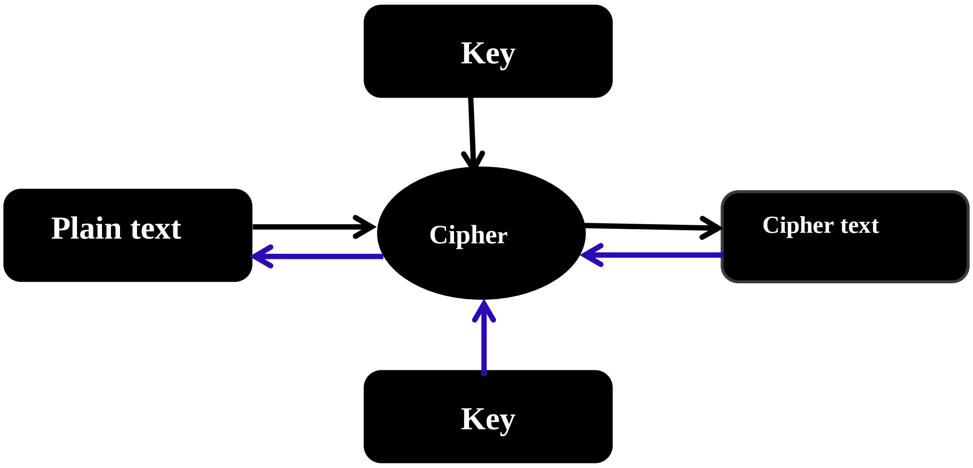


Figure 4. A simple graphic illustrates the concepts of encryption (flow of black arrows) and decryption (flow of blue arrows) methods

Numerous encryption methods are available for implementation in cloud computing, each presenting distinct advantages and disadvantages. Among the most prevalent techniques are symmetric-key encryption, wherein a single key, known as the symmetric key, is utilized for both encryption and decryption processes. This method offers notable speed and efficiency; however, susceptibility to key compromise poses a risk of data loss. Symmetric encryption encompasses advanced encryption standards (AES) that employ varying key lengths, such as 128, 192, or 256 bits, with corresponding private keys of identical lengths.

Alternatively, public-key encryption, also referred to as asymmetric-key encryption, utilizes two keys: a public key for encryption and a private key for decryption. While this approach boasts enhanced security and resilience against key compromise, it is characterized by slower performance and increased computational demands. Common asymmetric algorithms include RSA and Diffie-Hellman (Elliptic Curve Cryptography). Symmetric encryption systems typically outperform their asymmetric counterparts and offer advantages over asymmetric cryptographic systems.

Lastly, hashing algorithms play a crucial role in data integrity by generating unique signatures or fingerprints of data. Unlike encryption methods, hashing algorithms do not encrypt data but instead create identifiers that facilitate data verification and authentication.

Hashing algorithms are mathematical functions used to produce a unique identifier (called a hash) based on the content of a given input. These hashes can be used to identify and verify the integrity of the original data.

They are commonly used in applications such as passwords, files, and databases. The main flaws associated with hashing algorithms are that they are not collision-resistant and can be vulnerable to pre-image attacks. Collision-resistant algorithms work by making it difficult to find two inputs which produce the same hash. Pre-image attacks involve finding an input that produces a given hash, which could potentially allow an attacker to crack passwords or find other sensitive data. Additionally, some hashing algorithms are vulnerable to length extension attacks, which involve adding data to the end of a given input to create a new hash.

We present a recent survey regarding open issues associated with various security and privacy models in cloud computing. The survey highlights the advantages and inherent limitations of the methods proposed by the research workers. Table 1 shows various different proposed methods, along with their description, and advantages and disadvantages.

Table 1. Encryption methods, method of approach, advantages, and disadvantages

S. No	Proposed Encryption Method and Reference	Methodology	Advantages	Disadvantages
1.	Cross-user deduplication (Tang et al., 2018)	By identifying extra copies of data, it deletes redundant data. Therefore, only a single instance can then be stored.	a) Reduces space and bandwidth requirements of data storage services b) Most effective when applied across multiple users	a) Can only offer meaningful privacy guarantees with a limited toll on the resources
2.	Message-locked encryption (MLE) (Bellare et al., 2013)	It works by combining traditional encryption techniques with the added security of locking messages with a unique key	a) Better security b) Cost-efficient and faster reaction times when dealing with extensive data	a) Not widely available b) Not suitable for public-key encryption as it requires a special key c) Too complex
3.	Homomorphic encryption (Gentry, 2009)	Allows any third party to operate on the encrypted data without decrypting it in advance.	a) Supports multiple operations on encrypted data	a) Implementation is extremely slow, as a result, the total cost of ownership increases.
4.	Blind decryption (Al-Fayoumi & Aboud, 2005)	Decrypt cipher texts without having access to the associated private keys	a) Faster decryption and encryption b) Reduces the risk of administrators misconfiguring the system, so it is harder for malicious actors to gain access to sensitive data	a) Time consuming b) As this requires two-way communication between the sender and the recipient, attackers can use this two-way communication to intercept and modify the data

5.	File assured deletion (Tang et al., 2012)	It works by using a combination of a randomly generated key, an algorithm, and a cryptographic hash to protect the data and protects deleted data with policy-based file assured deletion.	a) files are reliably deleted b) Remain permanently unrecoverable and inaccessible c) This encryption is incredibly secure	a) Encryption algorithms used are often extremely resource intensive b) As encryption requires a dedicated key to unlock the data, if the key is lost or stolen, the data is rendered inaccessible even to its rightful owner
6	Elliptic Curve Cryptography (ECC) (Ullah et al., 2023)	ECC is based on the mathematics of elliptic curves over finite fields and is widely used in many protocols such as TLS/SSL, PGP, SSH, and others.	a) Security: ECC provides stronger security than RSA cryptography, making it more difficult to break b) Speed: ECC can operate with smaller key sizes than RSA, resulting in faster encryption and decryption times c) Simplicity: Compared to RSA, ECC is simpler to implement and has a smaller footprint, making it more suitable for smaller devices d) Cost: ECC is generally less expensive due to the smaller key sizes	a) Complexity: More complex to implement than RSA, making it more difficult for some developers to incorporate into their applications b) Limited Compatibility: Not as widely supported as other cryptosystems, making it harder for some devices to use c) Susceptibility to Quantum Computing: With the potential rise of powerful quantum computers, ECC may be susceptible to attack by these machines.

4. THREATS MODELS, THEIR MODUS OPERANDI, AND OPEN ISSUES

Threat modeling serves as a vital tool for organizations, offering a comprehensive overview of their security stance and enabling them to foresee, detect, and effectively counteract potential threats. By engaging in threat modeling, organizations can take proactive measures to safeguard their data, systems, and applications from malicious actors. The primary objectives of threat modeling encompass identifying pertinent security requirements, pinpointing potential threats and vulnerabilities, evaluating the severity of these risks, and prioritizing appropriate remedial actions. Given the tangible outcomes produced by threat modeling methodologies, many enterprises are embracing multiple approaches to fortify the protection of their critical data assets.

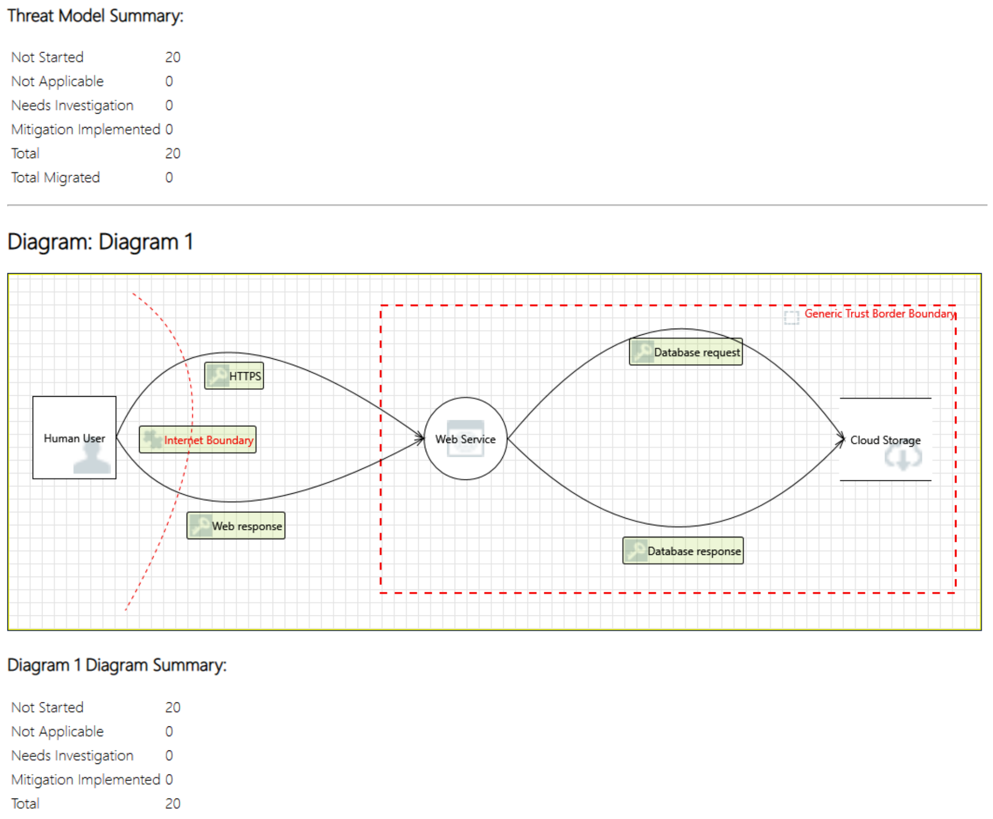
In the context of cloud computing, threat modeling facilitates the systematic assessment and mitigation of risks and vulnerabilities, aiding in the identification of gaps in existing security controls. Extensive documentation in the literature outlines various types of threat models, delineating their methodologies, strengths, and limitations. Table 2 provides an overview of these threat models, offering insights into their operational frameworks and highlighting pertinent open issues for further exploration and resolution.

Table 2. Various threat models, their modus operandi and open issues associated with them

S. No	Threat Model & Reference	Modus operandi	Open issues
1	Attack Tree (AT) (Chlup et al., 2023)	a) Identifying Attacker’s Goal - Root Node b) Decompose the Goal - Sub-Node c) Divide sub goals into Subtasks - Stepwise sub-Node d) Final goal computation when all	a) Unable to deal large sized networked systems b) Attack trees tend to be complex and it can be difficult to accurately model complex attacks c) Implementing an attack tree can be a

		nodes computed	complex process and requires a detailed understanding of the security threats d) Attack trees can be used to identify threats but they may not always identify all of them
2.	Attack Graph (AG) (Noel & Jajodia, 2017)	Assesses network configuration and vulnerability information of network by obtaining the entire dependency interactions of the information.	Unable to deal large sized networked systems
3	Likability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness and Non-Compliance (LINDDUN) (Deng et al., 2011)	With the aid of extensive privacy knowledge base, this model allows systematic support to elicit and mitigate privacy threats	It neither rank and identify nor define threats and vulnerabilities
4	Microsoft Threat Analysis and Modelling (TAM) (Scandariato et al. 2015)	To detect and assess potential threats, it uses data analytics and machine learning	a) Cannot provide assets determination and identification of vulnerabilities b) Despite the use of sophisticated algorithms and intelligent systems, the threat modelling results are sometimes inaccurate, which leads to exaggerated risks and false positives c) Expensive and difficult to use as this tool is highly specialized and requires skilled personal
5	STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) (Microsoft Corporation- The stride threat model, 2014)	By integrating security protocols in the development lifecycle itself, it is possible to assess the ensuing threats. To be precise, it's pre-defined framework	a) Because of the static nature of this model, it is unable to define new threats, vulnerabilities and privacy related issues b) Fails to adequately address privacy concerns or insider threats, or provide guidance on how to effectively mitigate risks
6	Threat modeling in pervasive computing (TMP) (Malik et al., 2008)	Different approaches have been proposed for threat modeling in pervasive computing. One method is to use attack trees to identify the possible attacks on a system and the associated vulnerabilities. Another approach is to use STRIDE	a) Lack of robust tools and frameworks for identifying and responding to threats b) Current tools and frameworks are often limited in their ability to detect and respond to threats, which limits the effectiveness of threat modeling c) Another challenge associated with threat modeling is the need to design processes that are both effective and efficient

To show the readers how the threat model works, we have downloaded the Microsoft STRIDE Threat Modeling Tool (TMT 2016) to guide them to carry out the threat modeling process in a few easy steps and presented those results as a case study. The threat model works on the following steps which include, selecting a model, drawing the diagram, identifying the threats, mitigating by adopting proper mechanisms, and finally validating the number of threats. TMT was created in a way that allows users to create data flow diagrams that are as straightforward as ABC by choosing elements from the Stencils Pane located in the right-top corner of the window. To quickly model threats, we have created a straightforward model.



Threat Model Summary:

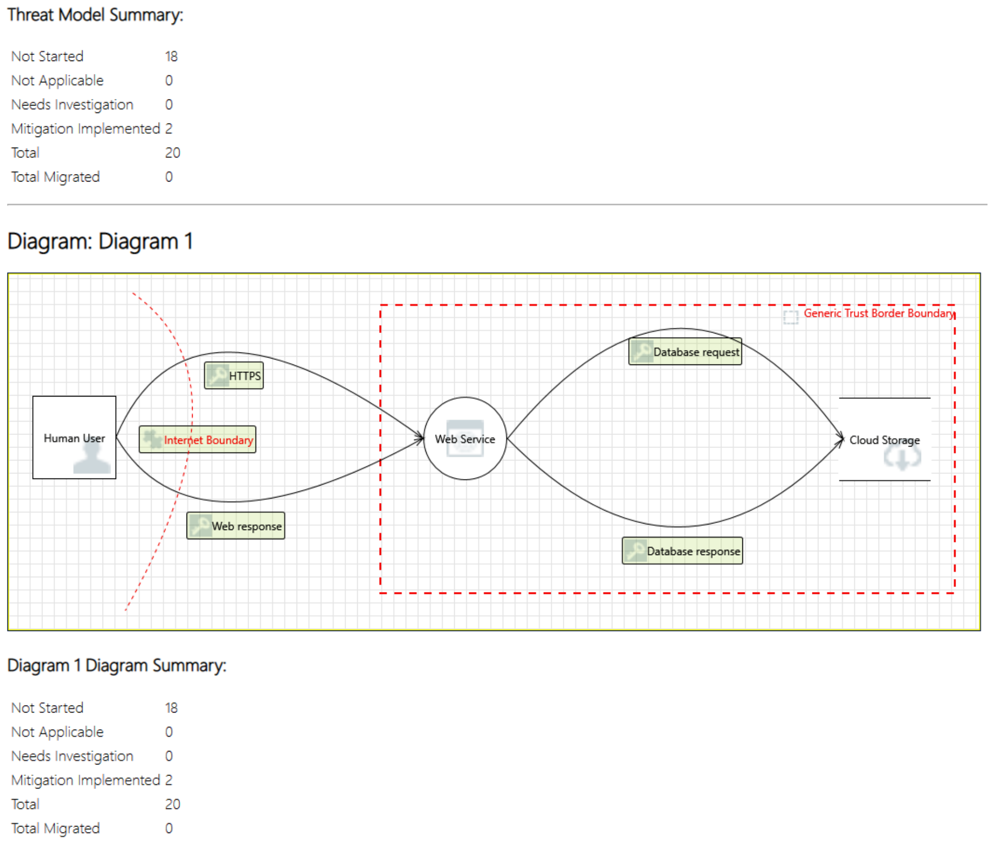
Not Started	20
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	20
Total Migrated	0

Diagram: Diagram 1

Diagram 1 Diagram Summary:

Not Started	20
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	20

Figure 5. STRIDE threat model screenshot and it can be seen that 20 threats (spoofing, denial of service, repudiation, etc.,) were simulated under no mitigations implemented category



Threat Model Summary:

Not Started	18
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	2
Total	20
Total Migrated	0

Diagram: Diagram 1

Diagram 1 Diagram Summary:

Not Started	18
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	2
Total	20
Total Migrated	0

Figure 6. STRIDE model screenshot and it can be seen that two threats were effectively sorted out under the mitigations implemented category

Figure 5 shows the screenshot of a simple case study using the STRIDE model, wherein a secure connection is established between a human user (left box) and cloud storage (right box) via a web service connection (middle box). The generated report shows that the threat model simulated a total of 20 (twenty) threats. Nevertheless, the situation changed and two threats were eliminated once a few mitigations were implemented, as shown in Figure 6. It may be worth mentioning here that, after users have kept the right mitigations in place, it is also possible to eliminate the greatest number of risks.

5. FUTURE RESEARCH SCOPE

As far as the future research scope is concerned, GPU-enabled cloud machines are offering substantial computing power at affordable prices. It is quite certain that a variety of devices and platforms will be able to implement various architectures and make use of state-of-the-art facilities of GPU-enabled cloud machines in real-time, so that huge offloading will be enhanced many folds, in days to come. To elaborate, days are not far away that research will focus to bring down all GPU-enabled cloud machines to low computing devices by leveraging the computing power of the cloud, so that greater penetration and awareness regarding cloud computing among the general public may occur. Serious research is being carried out along those lines by various research workers (Luo et al., 2018).

Further, it was designed as a smart agent for cyber-attack prevention and prediction using machine learning and honeypot systems that could deal the future attacks efficiently (Ahmadi & Salehfar, 2022). Another study conducted by researchers at the University of Pennsylvania in 2017, found that bio-inspired AI algorithms could detect suspicious activity on a computer network with near-perfect accuracy. These studies demonstrate that bio-inspired AI is a powerful tool for protecting users online. In a recent study, it was argued that privacy-preserving cloud computing technologies have enough caliber to provide efficient privacy to the cloud data and it was proposed a model based on bio-inspired AI and quantum-inspired AI-assisted privacy-preserving cloud (see figure 5).

6. CONCLUSION

Cloud Computing is a service model in which computer resources are delivered as on-demand, scalable, and virtualized resources through the Internet. Cloud computing is capable of providing dynamical scalability, reliability, high availability, and agility, to name a few. While the primary impetus behind the adoption of cloud computing lies in its economic advantages, specifically in reducing both capital and operational expenses. Particularly, organizations can benefit from cloud computing in several ways, such as increased accessibility, centralized data security, quick application deployment, and price-performance and cost savings. In addition, cloud computing offers flexibility, mobility, insight, increased collaboration, quality control, most importantly, disaster recovery.

On the other hand, it must be accepted that cloud computing is, still, prone to security and privacy breaches, most possibly due to the lack of practical adoption of adaptive mechanisms in combating threats. Though cloud-supporting technologies rapidly advancing like mushrooms, questions are being raised regarding the efficacies of those technologies to tackle effectively the ensuing threats, which is another important aspect that needs to be dealt with appropriately. Our literature survey revealed that different inefficient security and privacy solutions still exist that may mar the users to have secure and adaptive cloud environments.

Every individual organization must carefully weigh the benefits and hazards of cloud computing before deciding whether to adopt it and use it. Secondly, businesses should reconsider the quantity of data they gather, keeping only the absolute minimum amount of readable consumer data. With less data available for exploitation, consumers are exposed to less danger.

As far as the threat models are concerned, the cloud computing environment may offer more risks than threat models surely, despite the apparent reality that TMs give rapid flexibility, scalability, on-demand access, and others. To handle those risks, TM must be an ever-active and proactive process. Therefore, future TMs will need to be prepared to consider the effects of the cloud's distinctive traits. Unless otherwise stated, organizations, no matter how big or small, may have to face the dangers posed by the present and the ensuing threats.

References:

Agarwal, S., & Kaushik, J. S. (2020). Student’s perception of online learning during COVID pandemic. *The Indian Journal of Pediatrics*, *87*, 554-554.

Ahmadi, S., & Salehfar, M. (2022). Privacy-preserving cloud computing: ecosystem, life cycle, layered architecture and future roadmap. *arXiv preprint arXiv:2204.11120*.

Alharbi, Y., Rabbi, F., & Alqahtani, R. (2020). Understanding university student’s intention to use quality cloud storage services. *International Journal for Quality Research*, *14*(1), 313–324. https://doi.org/10.24874/IJQR14.01-20

Al-Fayoumi, M., & Aboud, S. (2005). Blind decryption and privacy protection. *American Journal of Applied Sciences*, *2*(4), 873-876. doi:10.3844/ajassp.2005.873.876

Al-Hajri, S., Echchabi, A., Ayedh, A. M., & Omar, M. M. S. (2021). The Cloud Computing Systems' Adoption in the Higher Education Sector in Oman in Light of the COVID-19 Pandemic. *International Journal of Evaluation and Research in Education*, *10*(3), 930-937.

Alsufyani, R., Safdari, F., & Chang, V. (2015, January). Migration of cloud services and deliveries to higher education. In *Proceedings of ESaaSA 2015-2nd International Workshop on Emerging Software as a Service and Analytics, In conjuction with the 5th International Conference on Cloud Computing and Services Science-CLOSER 2015* (pp. 86-94).

Bellare, M., Keelveedhi, S., T. Ristenpart (2013), Message-Locked Encryption and Secure Deduplication. In: Johansson, T., Nguyen, P.Q. (eds) Advances in Cryptology – EUROCRYPT 2013. EUROCRYPT 2013. Lecture Notes in Computer Science, 7881 Springer, Berlin, Heidelberg. doi:10.1007/978-3-642-38348-9_18

Bhardwaj, A., Garg, L., Garg, A., & Y. Gajpal (2020), E-Learning during COVID-19 Outbreak: Cloud Computing Adoption in Indian Public Universities. Computers, *Materials and Continua*, *66*, 2471–2492. doi:10.32604/cmc.2021.014099

Brahmanandam, P. S., Chakravarthy, K. K. J., Raju, G. R., Rao, N. S., Satyavani, M., Kumar, V. N., ... & Satish, L. (2020). Feasible Solutions and Role of Nanomaterials in Combating the COVID-19 Pandemic: A Preliminary Study. *Trends in Biomaterials & Artificial Organs*, *34*, 44–51.

Chlup, S., Christl, K., Schmittner, C., Shaaban, A. M., Schauer, S., & Latzenhofer, M. (2022). THREATGET: towards automated attack tree analysis for automotive cybersecurity. *Information*, *14*(1), 14. doi:10.3390/ info14010014

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, *16*(1), 3-32. doi: 10.1007/s00766-010-0115-7.

Dierks, T., & Allen, C. (1999). Rfc2246: The TLS protocol version 1.0. RFC Editor, USA.

Gao, F., Thiebes, S., & Sunyaev, A. (2018). Rethinking the meaning of cloud computing for health care: a taxonomic perspective and future research directions. *Journal of medical Internet research*, *20*(7), e10041. doi: 10.2196/10041

Gentry, C. (2009, May). Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing* (pp. 169-178). Presented at the Bethesda, MD, USA. doi:10.1145/1536414.1536440

Golightly, L., Chang, V., Xu, Q. A., Gao, X., & Liu, B. S. (2022). Adoption of cloud computing as innovation in the organization. *International Journal of Engineering Business Management*, *14*, 18479790221093992. doi:10.1177/18479790221093992

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of internet services and applications*, *4*, 1-13. doi:10.1186/1869-0238-4-5

Hori, M., Kawashima, E., & Yamazaki, T. (2010). Application of cloud computing to agriculture and prospects in other fields. *Fujitsu Sci. Tech. J*, *46*(4), 446-454.

Khan, S. S., & Tuteja, R. R. (2015). Security in cloud computing using cryptographic algorithms. *International Journal of Innovative Research in Computer and Communication Engineering*, *3*(1), 148-154.

Kushagra, K., & Dhingra, S. (2021). Cloud doctrine: impact on cloud adoption in the government organizations of India. *Journal of Science and Technology Policy Management*, *13*(4), 925-951. doi:10.1108/JSTPM-06-2019-0058

Luo, Z., Small, A., Dugan, L., & S. Lane (2018), Cloud Chaser: Real Time Deep Learning Computer Vision on Low Computing Power Devices. *ArXiv*. doi:10.1117/12.2523087

Microsoft Corporation. The stride threat model, 2014. URL http://msdn.microsoft.com/en-US/library/ ee823878(v=cs.20).aspx.

Noel, S., Jajodia, S. (2017). A Suite of Metrics for Network Attack Graph Analytics. In: Network Security Metrics. Springer, Cham. doi:10.1007/978-3-319-66505-4_7

Ramu, G., & Eswara Reddy, B. (2015). Secure architecture to manage EHR's in cloud using SSE and ABE. *Health and Technology*, *5*, 195-205.

Scandariato, R., Wuyts, K., & Joosen, W. (2015). A descriptive study of Microsoft's threat modeling technique. *Requirements Engineering*, *20*, 163-180. doi:10.1007/s00766-013-0195-2

Sowah, R. A., Ofori-Amanfo, K. B., Mills, G. A., & Koumadi, K. M. (2019). Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in artificial neural networks (ANN). *Journal of Computer Networks and Communications*, *2019*(1), 4683982. doi:10.1155/2019/4683982

Tantatsanawong, P., Kawtrakul, A., & Lertwipatrakul, W. (2011, March). Enabling future education with smart services. In *2011 Annual SRII Global Conference* (pp. 550-556). IEEE. doi: 10.1109/SRII.2011.63.

Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. (2023). Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. *Computer Science Review*, *47*, 100530. doi:10.1016/j.cosrev.2022.100530

Yang, Z., Liang, B., & Ji, W. (2021). An intelligent end–edge–cloud architecture for visual IoT-assisted healthcare systems. *IEEE internet of things journal*, *8*(23), 16779-16786.

N. Praneetha
KLEF University,
Vaddeswaram- 522 302,
India
nyshpranee@gmail.com
ORCID 0000-0002-7027-9516

S. Srinivasa Rao
KLEF University,
Vaddeswaram-522 302,
India
srinu1479cse@kluniversity.in
ORCID 0000-0002-6183-7088

P. S. Brahmanandam
Shri Vishnu Engineering College for
Women (A), Bhimavaram- 534202,
India
dranandpotula@svecw.edu.in
ORCID 0000-0001-9777-3496