Recent Advancements in Cloud Security Using Performance Technologies and Techniques

Vamshidhar Reddy Vemula  
 *Intalent LLC  
555 Republic Dr 425, Plano*  
 TX, USA 75074  
vvamshidharreddy1@gmail.com

***Abstract***— **This study examines the numerous approaches to cybersecurity and cloud computing offered by various authors in the past. Coverage includes cloud computing intrusion detection and prevention systems, cloud forensics and anti-forensics technologies, strategies for enhancing security and privacy in cloud environments, key management and cryptographic strategies, securing multi-cloud environments, cloud computing confidentiality, and distributed authentication and authorization schemes for big data sharing. These studies provide useful information on the most recent techniques used to safeguard private data, ensure cloud security, and improve cloud services. The study emphasizes the significance of robust security measures, data protection, and efficient administration strategies in a cloud environment that is constantly evolving. This study provides the foundation for future research and advancements on the topic of cloud security by contributing to a greater understanding of the sector's problems and solutions.**

***Keywords***— ***Cloud Security, Intrusion Detection, Prevention Systems, Cryptographic Strategies, Data Encryption, Patch Management.***

# Introduction

The flexibility, scalability, and cost-effectiveness of cloud computing have revolutionized how organizations operate in the modern digital world. As more businesses and individuals utilize cloud-based services for data storage, processing, and application deployment, it is impossible to exaggerate the significance of cybersecurity in this context. Due to the cloud's accessibility and lack of centralized control, it has become a target for both good and bad actors. This emphasizes the critical need for comprehensive cybersecurity solutions that can address the unique cloud computing risks. In this study, we investigate the expansive field of cloud security. We discuss the current methods used to address the complex security issues generated by cloud computing, as proposed by numerous authors and industry experts. preserving data and applications, detecting and preventing breaches, managing cryptographic keys, preserving confidentiality, and establishing secure service level agreements are some of the various aspects of cloud security. The overall objective is to provide a comprehensive overview of the proposed solutions to these problems.

Preventing and detecting intrusions are two of the most challenging aspects of cloud security. The inability of traditional intrusion detection and prevention systems (IDPS) to keep up with the sophistication of cyberattacks. Cloud-based intrusion detection is more difficult than on-premises detection due to the cloud's dynamic and distributed service landscape. Multiple authors, including Patel et al. (2013), have emphasized the importance of preserving cloud infrastructures against both external and internal vulnerabilities. This study examines the sophistication of Intrusion Detection and Prevention Systems (IDPS) in cloud environments. In order to increase the security of cloud infrastructures, we examine how ontology, self-management, fuzzy theory, and risk management could be implemented within IDPS. The research also examines how key management and cryptographic techniques enhance cloud security. Security, authentication, and authorization in the cloud require cryptographic keys. Best practices for key management include safe key generation, secure storage, regular key exchanges, and compliance reviews. In this article, we investigate the potential of Identity-Based Cryptography (IBC) to provide a distributed authentication and authorization framework for the secure sharing of vast quantities of data in the cloud. Threats occurs are malware, data threat, botnets, software vulnerabilities and SQL injection.

The concept of cloud-based privacy is another crucial area that requires your attention. Nataraj (2021) suggests using hardware-integrated trusted execution environments to safeguard sensitive data during processing in confidential computing. This method prevents security vulnerabilities such as root user compromises and memory leaks by encrypting all data in memory. We examine the prospective applications and functions of confidential computing in securing the privacy of cloud-based data. How service level agreements (SLAs) contribute to cloud security is also investigated. SLAs are legally binding contracts between a company and its consumers that specify the services to be rendered as well as any quality or security guarantees associated with those services. Our investigation into SLAs include such areas as service description, reliability, responsiveness, change management practices, and confidentiality assurances. We emphasize how SLAs can help create realistic expectations for all parties involved, reduce conflicts, and improve the security of cloud services. Ensuring confidence and adherence to regulations in the rapidly evolving, interconnected digital landscape of the twenty-first century necessitates rigorous security protocols, thorough data safeguarding, and efficient management, all of which are critical in the growing cloud environment. By providing a summary of the research conducted and expanding on the issues raised in the abstract, this paper intends to accomplish its objective. The abstract should provide a concise overview of the study's key findings, contributions, and main points so that readers can rapidly grasp its scope and significance.

# Related Work

*A. Research & Production Honeypots*

Honeypots are used by security analysts to lure intruders with fake versions of sensitive information (Kelly et al., 2021). Honeypots within a company's network are used by cybercriminals to locate and take data. When a hacker attempts to break into a network, they frequently leave digital traces that security personnel can use to thwart future attacks. Honeypots in production provide the overwhelming majority of information about cyber threats in the business world. Honeypots can be used by hackers to snoop on traffic, IP addresses, and user directories in live environments. Due to their adaptability and openness, production honeypots are widely recognized for exposing cyberattack vulnerabilities. In production, honeypots are not as effective as they are in testing. Research honeypots, on the other hand, maintain track of the methods hackers use to break into networks. Research honeypots, like production honeypots, use false data to entice hackers for the purpose of testing and refining countermeasures. Honeypots are used by both governments and programmers for research objectives. Research honeypots are more adaptable than production honeypots, which are typically utilized only within a specific network. Honeypots for research require more time and effort to put up. Fig 1 depicts the working of honeypots.

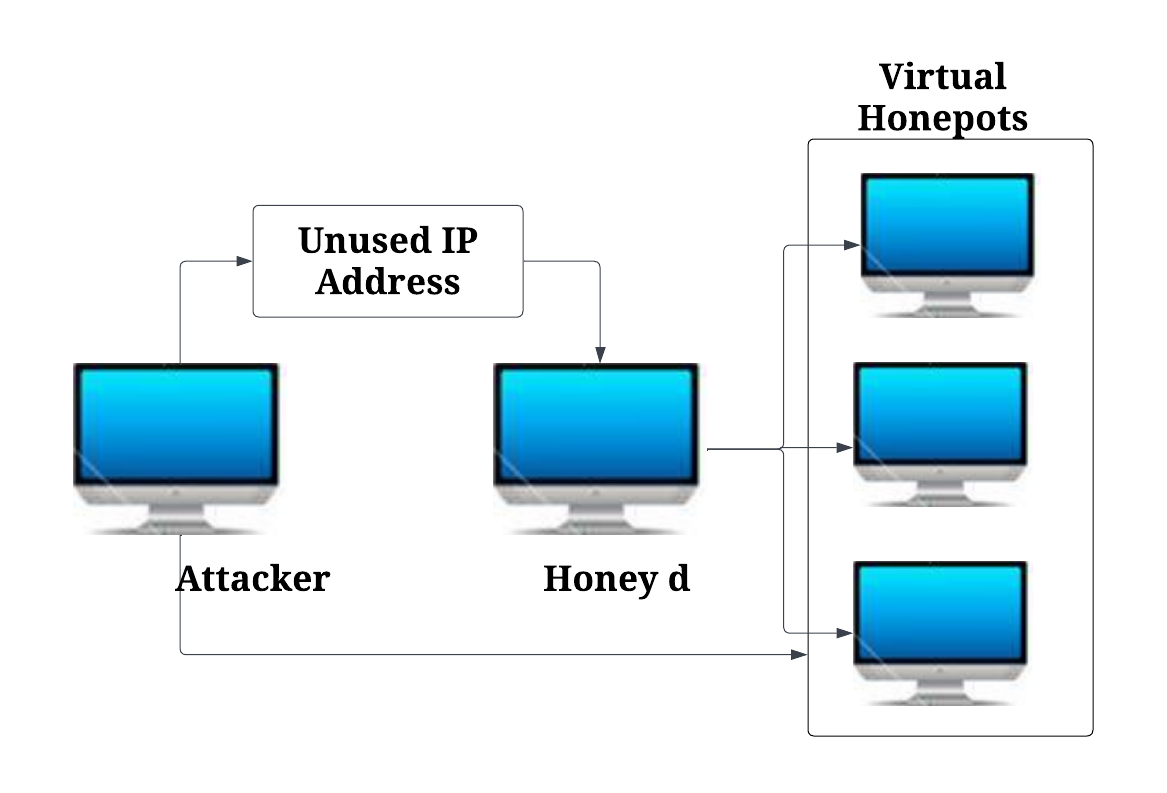


Fig. 1. Working of Honey D

Fortunately, honeypots provide additional information regarding vulnerabilities and attacks. While remaining connected to the demilitarized network, honeypots are protected from the rest of the network. Demilitarized networks enable honeypots to be remotely monitored without requiring access to the primary network. Using honeypots located outside the firewall, potential network threats can be investigated. Certain locations will be more appropriate for honeypots depending on the volume of traffic or the significance of the data. Honeypots must be entirely cut off from the rest of the organization's network. Honeypots are a technique employed by some hackers to spread disinformation. Honeypots are used by attackers as a decoy to obtain access to networks because they collect information about infrastructure threats. Honeypots were hosted on virtual computers because virus entries reset them, rendering them ineffective to assailants. Honeypots may have a high rate of interaction, a low rate of interaction, or be pure. High-interaction honeypots that mimic the actions of an actual system can be used to collect information on attackers. The server could be compromised and their actions monitored. True honeypots snoop on the victim's network. Honeypots are difficult to deceive attackers with (Chandra & Madhuri, 2015). Honeypots are counterfeit networks or systems designed to deceive and entice hackers. They contribute to the enhancement of network security through the provision of support to security professionals in their efforts to acquire threat intelligence, analyze attack patterns, and gather information on potential threats. Utilizing honeypots hosted in the cloud offers numerous advantages, such as enhanced threat detection capabilities, comprehensive security monitoring, and reduced risk.

*B. Intrusion Detection & Prevention System*

Cybercriminals are increasingly exploiting the distributed and open nature of the cloud and computers. Due to the open and unique nature of the cloud, commercially available intrusion prevention and detection systems are ineffective. This topic investigates the most recent Intrusion Detection and Prevention Systems (IDPS) in order to educate researchers on how to manage intrusion detection and prevention in the cloud. Ontology, self-management, fuzzy theory, and risk management are necessary for IDPS in cloud computing systems. With the same intent, attacks on a computer system may originate from both inside and outside the network (Patel et al., 2013). Attacks are undesirable events. It is possible for an intruder to gain illicit access to a system by altering the address of a computer. An IDS can detect and automatically detect intrusions. As a hardware or software device, an IDS can however detect and prevent intrusions.

Contrary to preventative systems, detection systems require material updates to assure safety. An improved network architecture could prevent "queen attack" attacks. Modify the target's host-based firewall to prevent intrusions. Eliminate weak spots and replace them with safeguards. By instructing the preventative system to distinguish between authorized and unauthorized environmental intrusions, false alarms can be reduced. Conventional IDSs process audit information from the cloud. When one component is compromised, the cloud as a whole is protected. An ontology unifies data and facilitates communication, whereas an autonomic management monitor ensures that the IDPS is always running the most recent software and hardware. Fuzzy Logic Risk Managers are responsible for, among other things, analyzing systems, identifying potential threats, assessing the severity of those threats, responding to attacks based on what they have learned, and optimizing available resources in real time. The functional layer can detect, evaluate, and defend against IDPS malice. Analysis of IDPS data exposes system vulnerabilities. Keeping a close watch on infrastructures worldwide. Network-based intrusion detection systems scrutinize network and application protocol data to identify malicious activity on disconnected networks and devices. Network-based dynamic packet inspection utilizing IDPS. IDPs in the host nation carefully monitor computer stability. Logs and subpar performance indicate IDPS issues within an application.

Increase the security of a network or system by monitoring for and recording anomalous activity in real time. Real-time IDPS attack data may be retrospectively analyzed. Detecting irregularities, mistreatment, and hybrid models. By keeping an eye out for indicators of abuse, it may be possible to predict the efficacy of future infiltration operations. We use machine learning, data mining, and statistical methods to identify anomalies. System events are required for TCP connection and CPU usage recording. The statistical method is capable of predicting the behavior of a population. Detection and training based on statistical profiles. Second, by adapting the execution strategy to the input, machine learning-based solutions can potentially increase the loop cycle's efficacy. Therefore, Marvok and Bayesian models should be utilized. Data mining utilizes correlation, new trends, changes, anomalies, and significant data relationships/structures to identify potential security vulnerabilities. In alarm management, quality enhancement and communication linkage are employed as methods. Additional context or vulnerability data may improve the effectiveness of alerts. Alarm correlation is intensively pursued in an effort to reconstruct crucial events from preliminary signals. The majority of intrusion detection systems will issue a warning before an attack. It is possible to combine multiple assaults into a single meta-alert. For the purpose of generating events, notifications are correlated. You may have an implicit, explicit, or conditional link to your security system on your devices. Data mining enabled the collection, sorting, and categorization of numerous notifications. The warning connotation is lost in a context that is implicit. This strategy enables security personnel to define warning pattern limits more precisely and verbally communicate complex attack scenarios. The semi-explicit method adds additional constraints to first-order formulations.

Its security systems can detect and thwart intrusion attempts. Both the wired public telephone network and the point-to-point analog line support dial-up. If the network topology or traffic patterns are suspect, wires may be compromised. Unbound mobile nodes organize themselves. The stand-alone IDPS, which detect intrusion independently on each node, the distributed IDPS, which detect intrusion cooperatively, and the hierarchical IDPS, which detect intrusion separately into clusters, are launched separately in multilayered networks into clusters where a head drives mobile agents IDPS and local nodes through large networks with a specific task. The characteristics of mobile agents are extremely diverse. Two sections comprise the IDPS hierarchical taxonomy. The first section focuses on the technology, structure, audit data analysis/collection, responses, and detection techniques utilized in unusual contexts. The procedure of creating an IDPS in the cloud is complex. Traditional IDPS rules are unchanging because node groups have ongoing demands and monitored systems remain inactive. The preponderance of administrators of cloud security have faster response times. Interactions with people dull down reflexes. A hostile cloud service provider may employ insider information to their advantage. The sharing of virtualization technologies and infrastructure exacerbates cloud computing's security concerns. Because of multi-OS virtual machines, hypervisors are vulnerable to unauthorized control.

*C. Technologies and Implementations Relating to Cloud Forensics and Anti-forensics*

According to Shackleford 2021, cloud computing forensics aids cybersecurity specialists. Experts in cyber security frequently encounter obstructions when attempting to safeguard sensitive cloud data. Modern technology enables forensic investigators to access and analyze cloud-based data and systems. Analysts and acquirers concentrate on three kinds of data when examining evidence. Examples include workload storage volumes, RAM, network packets for traffic analysis, and cloud event recordings. In terms of analysis and acquisition, cloud forensics have come a long way, but there are still significant issues. If the skeptics are correct, there must be a compelling reason to continue with the evidence. Using cloud forensic techniques and tools, security professionals can automate investigations. The process of capturing a disk image of a live instance is identical to that of a virtual machine. Consequently, IaaS cloud providers enable the snapshotting of virtual machine (VM) operations by their clients. Create a snapshot-based live analysis volume and attach it to a forensics workstation in the cloud or on-premises. Using the IaaS administration portal, clients can create copies of operating systems and data drives. Fig 2 depicts the Network topology diagram.

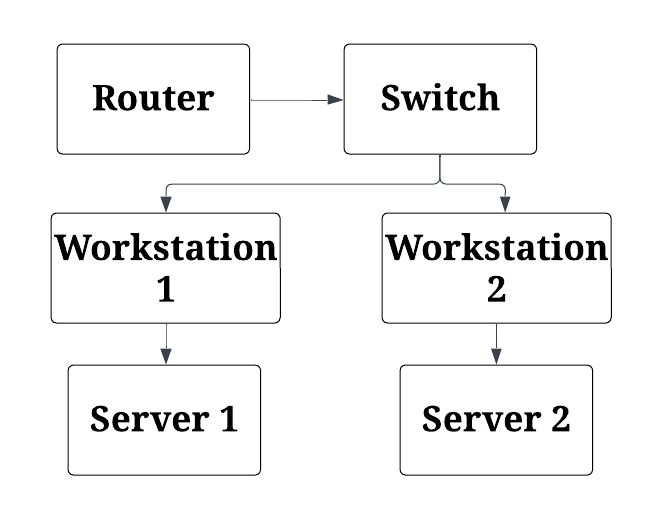


Fig. 2. Network Topology diagram

Every shared memory capture technique must have one. Accessing the operational memory of a local or remote instance necessitates a variety of techniques for cybersecurity professionals. Free, open-source notetaking software. An example of this is Google's Rekall. Hibernating processes is another way cloud systems save memory to local storage. The Google Cloud Platform security team constructs RAM disks for in-memory data. The majority of agent-based third-party systems, especially those serving enormous corporations, have migrated to the Cloud. Cloud-based systems frequently provide packet capture and network traffic monitoring for network forensics. Using flow log data for network traffic simulation. After incident report duties have been preserved, businesses must permit forensic cloud computing investigations. Included are the notion of leasing privilege access and the strategy for managing access and identities. Evidence collection and storage requires meticulous documentation. For a comprehensive cloud computing forensics program, logs from an integrity-monitoring storage environment are required. Analysis of multiple processes for automation is part of cloud computing incident reporting. Current duties include environmental evaluation, locating and designating suspect assets, collecting evidence, and cleaning. In a continuous environment evaluation, cloud-native technologies such as AWS config are utilized to examine resource security. Second, cloud network traffic anomalies are indicative of illicit activity. Automatically tagging assets with information is the simplest method for identifying those that are behaving oddly. The collection of evidence from disk, memory, local indicators, and compromise can be automated. Using cloud-based tools and programs, audit and log traces can be generated for monitoring and chain of custody purposes. Automating waste management and quarantine procedures enables quick, consistent responses to suspicious behavior.

*D. Enhanced Security & Privacy*

Duncan contends that in 2019 computation is more complicated than distributed systems. Cloud operations and novel Cloud interfaces are becoming increasingly methodologically difficult and complex. This article discusses confidentiality and safety. Better cloud privacy and security can be achieved through goal-setting, auditing issues, compliance with standards, a management approach, a lack of breath and accountability, technological complexity, management security attitude, measurement and monitoring, a threat environment, and a culture of security in the workplace. Inability or unwillingness to establish security objectives. Goals are the foundation of every successful strategy. Designing for security is crucial. Secondly, we must transition from rule-based to risk-based security using consensus and conformance auditing tools. A forceful and direct approach facilitates future compliance with standards. Although implementations may vary, conformance based on risk is preferred in cybersecurity. Due to their primary purpose, cybersecurity assessments cause anxiety. First, external auditors are mandated by law and have been shown to increase investor confidence. Compliance with industry standards and assessments of information technology systems are the second and third objectives, respectively. Cybersecurity management must evaluate the completeness and significance of audit traces. It's feasible that no configuration is required, since the framework has all you need for a seamless audit.

Cloud ecosystem interactions are complex and require attention. Cloud ecosystem management is an essential competency for managers. This facilitates threat assessment and mitigation. Privacy and security of cloud data may be affected by management techniques. If security and privacy parameters and management process constraints are implemented, the system may be secure. As technology becomes more complicated, the risk of misinterpreting value grows. The majority of decentralized information systems include a communication layer. The cloud enables actors to post more frequently. Instead, cloud brokers add new dimensions of complexity, risk, and opaqueness. Even with potentially hazardous default settings, cloud servers can send data faster than database-backed Web servers. Unfortunately, vulnerabilities are created because default settings prioritize usability over security. The majority of users are unaware that deactivating audit recording in the database's default settings may facilitate attacks. To maximize the number of errors found and resolved while preserving a forensic trace, it is necessary to manage Cloud technology-related concerns. Cybersecurity suffers in the absence of accountability. When the proper individuals have access to their data, their motivation to perform decreases. The cloud must be created with responsibility in mind. Cloud service providers require cybersecurity specialists to assist with SLA monitoring, administration, and negotiation. It can be difficult to quantify cloud services. Consequently, security management requires constant vigilance. Global cybersecurity groups attribute 85% of cloud and non-cloud data exposures to system design or victim ignorance. Prior to developing achievement metrics, security companies must first establish their goals. If management's security goals are continuously monitored, they may be compromised.

Reduce the number of user interfaces to improve the system's usability. Attackers are attracted to defenses with flaws. The code of the operating system is analyzed for vulnerabilities. Limiting the maximum quantity of executable code prevents both malware and data breaches. Increased internal access to virtual devices, according to cyber security experts, deters malicious actors. According to specialists, auditors may benefit from construction time planning. Keep your response brief and straightforward. Separating functions is advised by specialists. In public clouds, individuals share information, whereas in private clouds, hardware is shared between enterprises. The requirement for service isolation is crucial. Implementations of 86 protected mode and other hardware-enabled virtual memory make it easy to partition kernel services. The security of isolated processes is endangered by user permissions and mainframe configurations. Tools for paravirtualization and virtualization provide IBM hardware users with security. Docker for Linux compartmentalizes operating systems using virtual containers. In Docker Linux Containers, the kernel is shared among all users. Linux's namespaces and groups are utilized to isolate containers from one another. Containers are vastly superior to virtual machines. Internally, Google employs containers for virtualizing hardware and deploying multiple clouds. Hardware virtualization may provide isolation by means of uni-kernel, monolithic, and microkernel approaches. Disabling superfluous device drivers enhances cloud performance for Windows and Linux VM images by disabling unnecessary device drivers. Using a customized distribution of Linux could potentially reduce the amount of resources required to host virtual machines. According to experts, each microservice requires a dedicated virtual machine. This enables the development of fault-tolerant, extremely reliable systems.

*E. Application of Key Management & Cryptography*

Using cryptography to generate passwords must be secure. For data encryption, decryption, and authentication, keys are required. Businesses should implement key access restrictions to prevent unauthorized users from accessing the server and decrypting sensitive information (Encryption Consulting, 2021). The administration of keys includes the production of reproductions and the replacement of missing keys. Administration of Organizational Keys Standardization of cryptographic keys ensures safety. Here you will discover the root, master, and data keys. Secondary encryption keys are encoded using a 256-bit hardware security module and a master key. During data encryption or activities involving secret keys, encryption keys protect the confidentiality, authenticity, and integrity of the primary key. It is possible to encrypt files with either symmetric or asymmetric keys. The RSA and AES key sizes range from 128 to 256 bits. The practice of encrypting user data with a key is now feasible. Keys generated by a cloud-based key management system may be safeguarded by a robust security architecture and hardware security modules, made accessible to only authorized users, rotated frequently, deleted when no longer required, and monitored for use. Automatic endpoint updates, compliance records, high scalability/availability, regulatory compliance, and the key management lifecycle all benefit from lower operating expenses with cloud-based key management. To safeguard cryptographic key data, NIST, PCI, DSS, HIPAA, and FIPS all depend on key management. Essential for key administration are best practices. Hard-coded cryptographic credentials in open-source software pose a security concern. Second, least privilege necessitates the capacity to recognize and communicate with staff members. The key may only be used by those who have been granted access to it. This implies that only a small number of offenders will face severe penalties. Using hardware security modules (HSMs), on-premises cryptographic keys can be protected. Using automation, key re-use after encryption is avoided. Enforcing security key requirements assists with compliance and safety. Their actions limit the number of essential consumers. Through segregated key management, users can generate and employ their own keys to secure data.

*F.* Strategies for Securing Multi-Cloud Environments

(2022 Walker Forecast) Multi-cloud enterprises require service-wide security. To accomplish the desired level of automation and visibility, apply the prescribed procedure consistently to all cloud configurations. As intelligent and inexpensive as multi-cloud solutions may be, they present a labor management challenge. The complexity is compounded by the fact that each cloud operates autonomously. Compliance and security are ensured through centralized management and monitoring in the cloud. When hackers target multiple databases, they increase their possibilities of causing data loss and improper configuration. Multi-cloud strategies that employ a unified view of cloud data may facilitate the visualization, administration, and supervision of data. Cloud service providers can enhance cloud security by recognizing the shared responsibility of consumers and vendors. Numerous service providers and contracts can make multi-cloud installations challenging (IBM, 2021). Cloud governance protects multi-cloud environments. Thanks to multi-cloud governance, all standards, processes, people, and objects are under control. Thanks to inter-cloud observability, cloud security and management experts can maintain the safety of all clouds. Through multi-cloud management, teams can avoid access issues. Businesses must enhance their security and transparency as a final step. Through the consolidation of oversight and control over multiple cloud environments, multi-cloud administration enables the circumvention of access challenges. The implementation of standardized policies and procedures across cloud providers guarantees that exclusive access to confidential data is granted to authorized personnel and software. By implementing this integrated approach, the likelihood of security lapses is significantly reduced as unauthorized access is restricted, access management is simplified, and visibility is improved.

# Conidentiality in Cloud

Confidence in Computing User data transfers within the CPU enclave are encrypted (Nataraj, 2021). The enclave is only accessible to authorized applications and the cloud service itself. Confidential computing enables businesses to securely share data with cloud service providers of their choosing. Private computing is dependent on data-based protections. The unencrypted program memory stores vital information. Before, during, or after processing, an application's data might be compromised by a malicious root user incursion, a memory breach, or another vulnerability. CPU enclaves are a potential hardware remedy for computing's privacy issues. Code-level encryption keys provide a dependable execution environment. If the authorized code was compromised, the computed keys would be rejected by the trusted execution environment. The trusted execution environment will not decrypt private data cached in RAM when not in use. Rady and Ishmael's 2019 investigation Operating systems and cloud hypervisors do not have access to the restricted data. Certain user requests necessitate confidential computations. A trusted execution environment is used to guarantee the security of analytical computer processes, such as machine learning algorithms, business logic, and applications. Using confidential computing, businesses can collaborate to develop cloud-based solutions without disclosing sensitive information. A potential remedy for cloud services to safeguard user privacy is confidential computing. Distributed computing ensures the security of local data by synchronizing programs across multiple nodes and IoT devices (Martinez, 2013).

# Authentication & Authorization for Big Data

Li et al. say big data collection and distribution need a network. Name-based data discovery was the goal of Information-Centric Networking (ICN). Centralized professional mediation and digital certificates for data retrieval increase authentication and authorization traffic and data security. Identity-Based Cryptography (IBC) is best for decentralized user authentication and authorization. Safely publishing, obtaining, and initializing data is important for authentication and authorization. Li et al. 2022 propose accurate registration and NOAM broadcast for worldwide data retrieval.

Security and verification across the distribution chain. Key server startup, key generation, DSA, and object activation start it all. Even though NOAM caches across all domains, credible institutions may join the network. Phase 2 marketers use encrypted copy files to identify authorized AMs instead of a server and attribute-based criteria. IBS's error-proofing ensures correctness, while key chain techniques and CP-ABE's wide permissions increase efficiency. This implies many data updates with different periods are possible. The CP-ABE computer code is symmetrically encrypted before distribution. Expressive attribute-based policies and file lockbox keys (KEK) may create symmetric keys. The user chooses an IBS signature for the last data retrieval step. User authentication is common for data publishers and FDs. Distributed authentication and authorization benefits go beyond data security. The NOAM, DM, and AM DAAS hashes safeguard Big Data. An attacker may find the MIMA by altering AM, NOAM, and DM and comparing the result to the data hash value. Businesses trust DAAS due to NOA user, FD, and publisher authentication and secure ICN registration. NOA's entity ID cross-checking with IBS verifies users and writers' identities in DAAS. DAAS could validate FD users and publications. The publisher submitted symmetric-key-encrypted DAAS data for faster processing. The DAAS policy tree and user groups offer granular security permissions. Finally, DAAS changes publisher characteristics automatically [16], [17].

# Service Level Agreement Focuses on Security

A service level agreement (SLA) is a contract between a consumer and a service provider that specifies the parameters of their relationship. Both internal partners, such as an IT help desk serving employees, and external partners, such as a small business employing a network/IT/cloud provider, can engage into service level agreements. The contract outlines the expectations and responsibilities of both parties. In service level agreements, standards, not outcomes, are prioritized. Both service providers and their prospective clients must be aware of one another's expectations. In addition to alleviating tensions, agreements also enhance service quality. The agreements' emphasis on internal problem-solving techniques to meet customer demands is a significant selling point (The National Cybersecurity Society, 2022). SLAs consist of a service's definition, dependability, responsiveness, problem reporting, change management, monitoring, reporting, credits, kick-outs, and statistics. Our services include security consultation, network configuration, backup and storage space, vulnerability monitoring, and upgrading. Default execution location for the service must be specified. The service level agreed upon for weekdays is 99.99%, while the level agreed upon for weekends and evenings is 99.9%. Agreements guarantee 24-hour accessibility. Describe the process of escalation, who to contact, and how to report issues. Accounting for Change is the method by which new versions of a service are made available. After service requirements have been met, the agreement may be modified to accommodate client needs. Depending on the service standards in place, different parties may monitor and report to consumers. After a service failure, consumers may receive a credit or be expelled. The contract excludes cataclysmic incidents that could cause service interruptions. Additionally, information specifies who has access to it, how to reach it, and its location. Our service level agreement safeguards your data regardless of whether you encrypt it, transfer it to another provider, manage its lifecycle, or delete it.

# Results

Table 1 Metric value of each method

|  |  |  |
| --- | --- | --- |
|  | **Metric** | **Value** |
| **Honeypots [8]** | Detection Rate | 89% |
| **IDPS [4]** | Intrusion Detection Time | 4.7 seconds |
| **Cloud Forensics [13]** | Investigation Automation | High |
| **Confidential Computing [11]** | Data Encryption | Secure |
| **SLA [14]** | Service Uptime | 99.9% |
| **Key Management [6]** | Key Rotation | 45 days |

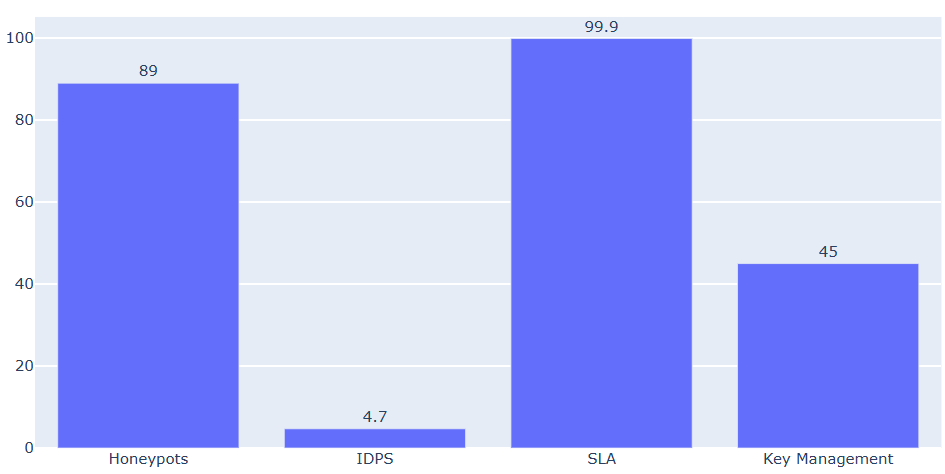


Fig. 3. Metric value of each method.

The Table 1 and Fig 3 provides essential indicators for various cybersecurity approaches. Honeypots have an 89% detection rate, while IDPS (Intrusion Detection and Prevention System) asserts a 4.7 second detection interval. Cloud forensics is distinguished by its extensive use of automation in the investigation process. On Confidential Computing, data is encrypted to a "secure" level. The SLA guarantees that the service will be available 99.9 percent of the time. In addition, Key Management requires a new set of keys to be distributed every 45 days. This type of metric indicates how effectively these safeguards prevent damage to digital assets.

Table 2 Key concepts, strategies and technologies

|  |  |
| --- | --- |
| **Concept** | **Use** |
| **Encryption** | Protects data in transit and at rest |
| **Identify and Access Management (IAM)** | Controls user access and authentication. |
| **Multi-Factor Authentication (MFA)** | Adds an extra layer of security to user logins. |
| **Virtual Private Cloud (VPC)** | Isolates network traffic within the cloud. |
| **Security Information and Event Management (SIEM)** | Monitors, detects and responds to security events. |
| **Zero Trust Architecture** | Never trust and always verify user access. |
| **Cloud Access Security Brokers (CASB)** | Monitors and secures data in the cloud. |
| **Patch Management** | Keeps software and systems up to date. |
| **Data Loss Prevention (DLP)** | Identifies and prevents data breaches. |
| **Intrusion Detection and Prevention Systems (IDPS)** | Detects and mitigates network threats. |

# Conclusion

Due to the dynamic nature of cloud computing, comprehensive, proactive security measures are required. Our analysis of extant methods presented by numerous authors and professionals highlights the critical need to address a variety of security issues, including intrusion detection and prevention systems (IDS/IPS), key management, confidentiality, and service-level agreements (SLAs). As more businesses adopt cloud computing, it is imperative that they take the necessary security precautions. Clearly, effective risk management requires a combination of cutting-edge technology, rigorous guidelines, and vigilant monitoring. By keeping apprised of cloud security advancements and best practices, businesses and individuals can confidently navigate the ever-changing digital world.

# References

[1] Montasari R (2017) An overview of cloud forensics strategy: capabilities, challenges, and opportunities. Cham, Strategic Engineering for Cloud Computing and Big Data Analytics. Springer, pp 189–205

[2] Freet, David, et al. (2015) “Cloud forensics challenges from a service model standpoint: IaaS, PaaS and SaaS.” Proceedings of the 7th International Conference on Management of computational and collective odelingnce in Digital EcoSystems

[3] Zargari, Shahrzad, David Benford (2012) “Cloud forensics: Concepts, issues, and challenges.” 2012 Third International Conference on Emerging Intelligent Data and Web Technologies. IEEE,

[4] Chandra, N. & Madhuri, S. (2015) Cloud Security using Honeypot Systems. International Journal of Scientific & Engineering Research.

[5] Duncan, B., Bratterud, A. & Happe, A. (2016) Enhancing Cloud Security and Privacy: Time for a New Approach? Research Gate.

[6] Encryption Consulting (2022) The importance of Key Management in Cryptography.

[7] IBM (2021) Multi-Cloud Solutions.

[8] Kelly C., Pitropakis N., Mylonas A., McKeown, S & J. Buchanan A Comparative Analysis of Honeypots on Different Cloud Platforms. Sensors.

[9] Li, R., Asaeda, H., Li, J. & Fu, X. (2021) A Distributed Authentication and Authorization Scheme for In-Network Big Data Sharing. Elsevier.

[10] Martinez, J. (2013) Privacy and Confidentiality issues in Cloud Computing architectures. Elsevier.

[11] Nataraj, N. (2021) Confidential Computing. IBM Cloud.

[12] Rady, M. & Ishmael, R. (2019) Integrity and Confidentiality in Cloud Outsourced Data. Ain Shams Engineering Journal.

[13] Shackleford, D. (2022) Cloud computing forensics techniques for evidence acquisition. Voodoo Security.

[14] The National Cybersecurity Society (2022) Service Level Agreements (SLA).

[15] Walker, A. (2022) Keys to Securing Multi-cloud Environments. Tech Beacon.

[16] K. R. Dalal and M. Rele, "Cyber Security: Threat Detection Model based on Machine learning Algorithm," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2018, pp. 239-243.

[17] M. Rele and D. Patil, "Supervised and Unsupervised ML Methodologies for Intrusive Detection in Nuclear Systems," 2023 International Conference on Network, Multimedia and Information Technology (NMITCON), Bengaluru, India, 2023, pp. 1-7.