Survey on Enhanced Security Control measures in Cloud Computing systems

Haider Hadi Abbas1, Zahraa A. Jaaz2, Israa Al_Barazanchi 3, Haider Rasheed Abdulshaheed 4

1Computer Technology Engineering Department, Al-Mansour University College (MUC), Iraq, https://ORCID.org/0000-0002-0724-7829
2College of Science - Computer department - AlNahrain University, Baghdad
3,4Baghdad College of Economic Sciences University, Baghdad - Iraq https://orcid.org/0000-0002-6798-6295

2,3College of Computer Science & Information Technology, Universiti Tenaga Nasional (UNITEN), Malaysia
1haider.hadi@muc.edu.iq, 2zaj@sc.nahrainuniv.edu.iq, 3Israa44444@gmail.com, 4haider252004@yahoo.com
*Corresponding author: Israa44444@gmail.com ; israa.albarazanchi@baghdadcollege.edu.iq

Abstract. Cloud Computing System is an internet based network of systems that provides a wide range of services to various companies and individuals, creating a digital environment for business progressing for a better world. Cloud Computing delivers a variety of services like remote storage, database management, applications and software, and high power computing performance, all these can be easily attained by subscribing to the cloud service, such that even from a low end PC system, any high end software can be run easily through means of internet. But, providing security to all of these services and stored data of private organizations has always been a challenge. Once a cloud server has been hacked, or an intruder has authorized himself into the server, he can simply sabotage, steal or misuse any sort of information of the client companies stored in within the server’s database. There are many ways to provide security to the different parts of the cloud, some methods are impenetrable, while some are fragile and can be broken through. This paper focusses on the various aspects of the cloud and its security functionalities, and how these security functionalities can be improvised. Some security measures can only protect the cloud by updating and regulating their terms and conditions, and some measures include various authorization methods and regularized access to cloud services.

Keywords — cloud computing, cloud security, cloud privacy, security enhancement

1. Introduction
With the advancement of cyber technology, cybercrimes are rapidly growing and to protect the cloud system is more than a priority for the cloud system itself to protect its client’s information and protect all of its own infrastructure, as obtained from existing systems [1]. The paper explains the existing technologies through the various cloud types and service models, and the major security threats that occur and how to improvise the security methods for better protection of all resources within. The enhanced security techniques are explained further on and how they provide better security is detailed for easy adaption on a practical cloud system. The security enhancements progress around two different basic techniques, the first technique is to update and regularize the terms and conditions for usage of a
cloud company’s services. The second technique is to enhance and hybridize previous methods for better control and liability to clients. The terms and conditions opted by a cloud company is a basic protection scheme that allows the client companies to access and use the cloud space, but permits them from abusing the services or the server itself by properly limiting their access at specific areas and functionalities as bound by the terms and conditions. This technique will prohibit the user’s access to various other areas of the cloud space, except their own virtual system as provided by the cloud. This technique works well, if the client uses the cloud for storage space, certain pre-opted software and for high end functionalities. But for services like databases, emails, hybrid cloud connect, mixed public-private areas and other such services, where the client or the hacker has too many options and areas to access and violate the terms. For such services, it will be too late to identify the violation and the harm would have been caused [2]. The second technique is to adapt to new and optimized methods of secure access for better of cloud resources, from the existing systems. Some of the optimized and enhanced techniques are explained later on in this paper. Such techniques can be employed for any type of cloud system with any service model and can be remodelled to suit the client and the cloud system better.

A. Cloud Computing
Cloud Computing system is a structure of multiple networks interconnecting various resources and facilities of the cloud and the client. There are multiple ways and techniques on how a cloud system is organized [3], and how security issues may arise from it. The diagram below represents how a client can access the cloud system and his require service or resources through means of internet, through secure authentications. While certain public clouds do not require authentication, rest of the cloud types require authentication for security and privacy. The cloud space refers to every parameter and units that fall under the cloud system and its control.

![Cloud Computing System](image)

**Figure 1. Cloud Computing System**

B. Cloud Architecture and Engineering
The cloud architecture is the base structure upon which a cloud system is built upon, it is through cloud architecture that every component of the cloud system is placed where it is supposed to be placed to benefit the cloud system, dependant on the purpose of the cloud space. Cloud Engineering is the methodology of bringing in engineering concepts and ideals to standardize, commercialize and improvise cloud computing systems and applications and help in the building of cloud architecture and governance over cloud components and structure with the clients.

1.1. Public Cloud
A public cloud is a space or a service that is provided for public usage. This type of cloud service is provided for individual or a group of users rather than a client organization. Examples of such public clouds are AWS Direct Connect, Amazon Elastic Compute, Google AppEngine, IBM’s Blue, Microsoft Azure and Salesforce Heroku. The problems with the public cloud are that it often experiences outages and storage loss, due to the excessive public usage. The other security issues are inadequate separation of user boundaries, loss of privacy and data hacking of premium clients.
1.2. Private Cloud
A Private Cloud is a cloud space or service provided to specific individuals or certain groups of people, mostly a private cloud exists within a public cloud with a certain level of isolation. The only security issues in this deployment method is the breaking of this isolation boundary that separates the public and private cloud. This may cause severe data stealing which will further cause more security massacres on its own way. Other private clouds are cloud spaces provided to client organizations.

![Figure 2. Public Cloud System](image)

1.3. Hybrid Cloud
A hybrid cloud is a cloud space or service that is a mixture of private cloud, public cloud or other third-party internal cloud spaces. This can be deployed as a single system, or multiple cloud platforms can be bridged together to form a hybrid cloud space. The security issues for this type of cloud system can happen through any multiple ends of any component of the hybrid, the problems arising in this type can only be reduce by taking security measures on singular systems within the hybrid cloud [4]. The diagram below depicts a hybrid system, where client1 can use only the public cloud, while client 2 can access both the public and private cloud, and both these clouds are managed by the cloud provider.

![Figure 4. Hybrid Cloud System](image)
1.4. Community Cloud
A community cloud is a cloud space or service that is provided to a group of client organization that are working together as a community. Community clouds offers the same service to many different clients over a set of common service models. This works best for companies that are working towards a common goal, or companies that have evolved out of a single parent company. Community clouds can be implemented internally [5], or externally over multiple server point or through third-party cloud companies. This cloud type offers a lot of transparency, and the security issues that occurs here are mostly through internal sources, or attacks from unknown third party intrusions.

![Figure 5. Community Cloud System](image)

1.5. Distributed Cloud
A distributed cloud is a cloud space that is distributed over many geographical locations, this is mostly preferred for companies having its branches worldwide. Distributed means spread across, in the field of cloud computing it means spread across multiple systems placed over multiple locations. It also works for clients who operate and access the cloud using multiple devices and interfaces [8, 13]. The singular system components have secular access control and access priorities set to it, that certain part of the system won’t have the ability to access a specific component within the system, but it able to access different other points within the cloud space as per its priorities and access provided. A distributed cloud will mostly be implemented internally, through internet, at rare occasions through third-party cloud sources. The majority of attacks on distributed clouds occur through internal system sources, or directly through internet.

![Figure 6. Distributed Cloud System](image)

1.6. Multi Cloud
A Multi Cloud is a big, diverse cloud environment supporting and hosting multiple cloud systems, over a huge structural network of varied cloud components and sub systems. Any cloud server can be interconnected with another cloud system to form a multi cloud, allowing greater access for a client system from one end of a cloud system, to access data at another end of another cloud system. The security issues are diverse, and the system can only be secure, by securing every single component end of the system.
1.7. Big Data Cloud

Big Data Cloud are huge cloud spaces specifically used for storing immense amount of data, and the need to access it right away, whenever it is needed. These clouds use multiple software framework to effectively store huge amounts of data in a specific pattern of clusters, enabling it to be easily accessed through cloud space. Big Data Cloud are used for MNC’s and big IT companies that processes tons of data every day, it is through this cloud space, and business process development have been a great hit. The issues with this cloud space is that, it requires large amounts of hardware resources that are used in clusters and when there is an attack or a system failure the entire data in a cluster might be lost, hence it requires multiple backup systems and proper maintenance of the entire server every once in a while.

1.8. HPC Cloud

High Performance Computing (HPC) Cloud is a cloud service that provide high end computing hardware resources to be used by client through internet. These are for companies that require large amounts of computing performance, and using internal hardware resources might not be enough to process all data. With the improving technological field it is not possible to drag high end hardware sources to every work locations and HPC cloud can be used to run high end software on a low end system through HPC cloud. There are not much security issues here, the only risk is through attackers who log in as a client, and might use the cloud to steal data, send spywares across the clients or disable a part of the cloud system.

1.9. Cloud Service Models

A cloud space provides many kinds of service, a cloud system is organized and its architecture built according to the services it provides. Each service has its own model of deployment, such service models are explained below with regards to priority. The architecture of a cloud system has to be built depending on the various types of services it provides, the overall system has to be well adequate to support the services that it has to provide.

- **Infrastructure as a Service**
  
  This provide infrastructure as a service to the clients, an infrastructure may contain high level API’s for use of other resources within that infrastructure like hardware resources, data partitioning, storage,
computing resources, security and backup services. With this model, any part of the cloud’s infrastructure can be shared [6].

- **Platform as a Service**
  This model provides clients a platform to run all computations, storage, backup, security and all other kinds of computing usage and supporting resources and storage. This allows customers to remotely operate their software and information from anywhere in the world, as in [7].

- **Software as a Service**
  This service model provides a software [8] as a product or service, this works on a subscription basis where the customers can upload their project to the cloud system and the cloud resources to run the software and work online. The common examples of these are google play apps, rebus farm and G suite.

- **Function as a Service**
  This service model provides customers to benefit by allowing them to develop, debug and run application functionalities without having a need to have their own superior complex hardware architecture and infrastructure. All other service models fall within these basic model types, at most of the times more than one service model is opted for a cloud system. The client’s On-premises contains all the infrastructure and hardware in a traditional way, the different service models and the services managed by the client is marked in blue, while the vendor managed is marked in red. Table 1 shows the Management of the various Service Models in accordance to the client and the cloud and table 2 shows the Comparison of Service Models based on their basic advantages and disadvantages. The tables, table 1 and 2 are in correspondence with the journal ‘Future Generation Computer Systems’, explaining parts of the different services the cloud has to offer [2].

### Table 1: Management of Service Models

| On-premises | IAAS | PAAS | FAAS | SAAS |
|-------------|------|------|------|------|
| Functions   | Functions | Functions | Functions | Functions |
| Applications| Applications | Applications | Applications | Applications |
| Data        | Data | Data | Data | Data |
| Runtime     | Runtime | Runtime | Runtime | Runtime |
| Middleware  | Middleware | Middleware | Middleware | Middleware |
| O/S         | O/S | O/S | O/S | O/S |
| Virtualization | Virtualization | Virtualization | Virtualization | Virtualization |
| Servers     | Servers | Servers | Servers | Servers |
| Storage     | Storage | Storage | Storage | Storage |
| Networking  | Networking | Networking | Networking | Networking |

### Table 2: Comparison of Service Models

| Service Models | Advantages                                                                 | Disadvantages                                                                                      | Cloud Providers                                                                                   |
|----------------|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| IAAS           | Extremely Cost Effective comparing with on premises infrastructure, highly flexible and highly scalable[2] | 1. Costlier than other service models. 2. Management of infrastructure falls on client. Privacy Issues may occur, and compromise confidential projects | CSC, GoGrid, IBM, Amazon Elastic Compute CCloud, OpenStack, Rackspace, Savvis, Bluelock, Citrix and VMware |
| PAAS           | Effective on developing Applications, saves a lot of time and money. Scalable. |                                                                                                   | Salesforce, SAP, Intuit, Amazon AWS, Google Apps, Netsuite, IBM, WorkXpress and Joyent             |
2. Security and privacy Issues
One of the primary concerns of cloud based systems is to provide security [9] and privacy to their clients. All sorts of security threats and privacy issues are listed accordingly further below.

a. Security Attacks
   • **Denial/Restriction of Services and Access**
     This form of attack prevents a client or the clouds maintenance sector from accessing a service or any part of the infrastructure.

   • **Insider Threats**
     This attack is done from the user/consumer side, where an employee abuses the system or attack was made due to an employee’s negligence.

   • **Phishing and Social Engineering Attacks**
     This attack happens mostly on public clouds, where a consumer tries to steal information of another consumer by hacking or performing a security override such that the system wouldn’t identify the hack, or by recreating the cloud’s identity. This attack can be prevented by providing specific limits to a consumer’s cloud space, doing this prevents a hacker from accessing other’s data by separating it’s user’s cloud space from each other. Other phishing attacks can’t be prevented, but it can be identified by using spam filters both for an individual or an organization.

b. Security Vulnerabilities
   • **Data Security**
     A cloud system that has failed to update its security in regards with the current trends will easily suffer security threats, these kind of systems can be easily hacked or abused.

   • **Shared Cloud Computing**
     Different cloud systems working in unison will have different types of security systems, and when working in synchronization will cause unnecessary system vulnerabilities [13, 14].

   • **Expertise of IT staffs**
     Employee negligence are also a primary problem for insider threats and social engineering attacks, the better expertise an employee has over the cloud system the better security measures that they will follow [14-17].

   • **Business Continuity and Disaster recovery**
     Once recovering an attack, the client’s business has to continue without facing any blackout and the disaster recovery measures should have a secure infrastructure and multiple backup systems. Failing to do so, it will take more time and money to continue their digital business and at times the recovery itself might fail.
c. Privacy Issues

- **Data Loss and Inadequate Backups**
  Privacy and data should be secured confidentially as per client’s needs and post a security attack, the data recovery might not be possible. So, for privacy reasons, the data should be uniquely encrypted and should have multiple backups in case of a failed recovery.

- **Non-compliance with regulatory mandates**
  Due to negligence, client may not follow certain cloud’s policies and might not be able to access a particular services or a storage.

- **Loss of control over IT services**
  This is an internal system problem, where the entire cloud system is not properly updated in concern with its growing client base and their service and storage consumption. Such an irregularity might prevent or withhold a client from accessing a service. To prevent his, the cloud system has to be auto updated whenever a change or addition of services/storage is brought on it.

The table below represents the major cloud attacks that happened over the years, according to the year it happened.

Table 3: History of Major Cloud Security attacks

| Year | Cloud Company                        | Product or Service Offered               | Description of the attack                                                                 | Severity of attack |
|------|--------------------------------------|-----------------------------------------|------------------------------------------------------------------------------------------|--------------------|
| 2010 | Microsoft                            | Business Productivity Online Suite      | This attack allowed non authorized users of the cloud to view certain employee contact illegally | Low                |
| 2012 | Dropbox                              | Cloud Storage                           | The security breach, allowed hackers to steal around 68 million accounts and all of its credentials | High               |
| 2013 | Yahoo                                | Yahoo                                  | The attack claimed a massive 500 Million user credentials and all personal details and storage | Extreme            |
| 2014 | Apple iCloud                         | Cloud Storage                           | The attacks compromised personal storage of high profile targets and celebrities, and leaked it online | Low                |
| 2014 | Home Depot                           | Home Depot Sales terminals              | The attack sabotages the point of sales terminals, directly affecting 56 million credit card number. | Extreme            |
| 2016 | National Electoral Institute of Mexico | Confidential Records – Government based | The attack compromised 93 million voter registrations records and made them publicly visible | High               |
| 2012-2016 | LinkedIn | LinkedIn Network                     | The attack on 2012, where 6 million user emails and password were set for sale on a dark web forum. In 2016, around 167 million user credentials were again displayed for sale. The breach claimed 143 million credentials, their credit card numbers, personal documents and identity proofs | High               |
| 2017 | Equifax                              | Equifax Firms                           |                                                                                           | High               |
3. Security Enhancements techniques

d. Biometric Authentication

This is one of the most secure ways of logging in to the cloud system [10], this is mostly preferred for cloud services deployed for high security and confidential services and storage. The authentication is done by storing the biometric information of a person within the cloud system, and every time the person tries to access the server, the biometric information is cross checked. The biometric can be anything from fingerprint, thumb print, face detection, retinal scan to blood DNA scan, depending on the scan device and the biometric signature used. On recording the fingerprint scan, the person’s heartbeat level can also be scanned. In case of threatening and forced biometric authentication, the heartbeat level will be high and the access can be denied for high security purposes.

![Flow-Diagram of Biometric Authentication System](image)

Fig 9: Flow-Diagram of Biometric Authentication System

e. Random Access Key

This is one of the simplest security system, where the user is provided a personal pass key every day, and the access is only allowed by using the updated pass key. So, by constantly resetting the pass key every day and by providing the passkey to the user’s digital workspace or work email, and by tracking the workspace or email log in IP address and location, the user can be easily identified and anyone try to hack in will be identified and blocked right away. Using such a system prevents anyone without an access key from any kind of access that can be provided by the cloud for its client and employees.
f. Data Encryption and Backup Systems

A cyber-attack or a system vulnerability can cause stored data to become corrupted. To prevent such events and secure data [9], it is obligatory to encrypt data and have multiple data backup systems. Encrypting data allows data security, and only the client can decrypt and use the data further. In case of data corruption or destruction, multiple remote backups are to be sustained by the cloud system. Multiple backup systems already exist in practice, but the original data is backed-up without any encryption and still lies a potential weakness for the client’s privacy, that is why it is necessary to encrypt data even on backing-up. Data encryption is the method in which the data is encrypted or compressed in a unique encryption method rather than the standard encryption methods will prevent anyone from decrypting the original data without knowing the encryption method and it is utmost important to generate unique encryption techniques.

---

Fig 10: Random Access Key Method Map

Fig 11: Data Encryption and Backup System
g. Employee Awareness
The best way to eliminate insider threats is to reduce employee negligence and constant supervision. By subjecting the employee through the rules and regulations of the cloud, process protocols and security protocols, they can be made more aware and can prevent insider threats and also remove the possibilities of becoming a victim of the cybercrime.

h. Security Audits and Upgrades
A security system is only made strong by considering the ways of hacking access into it. When a man can make it, a man can break it. So, by constantly updating and upgrading the security system [11]. Technology is upgrading from time to time, and along with the advancement of AI systems, it is necessary to upgrade one’s system to ensure security for the clients and their data.

i. Observations
With the technology constantly upgrading, it becomes harder and harder to protect a cloud system. Anyone can learn hacking and can break through a simple cloud system. It is always necessary to redefine a security system from any and every security attack operated over it. By constantly and consistently observing various attack methods, a system can be made stronger and almost inaccessible. From the enhanced security methods listed on this paper, it is observed that the biometric authentication method served utmost security for the cloud space and of the client and the data encryption and multiple backup system served the best prevention for privacy attacks and issues.

j. Conclusion
With the fact that it is necessary to protect the cloud system from viable threats, but greater is the compulsion to constantly and consistently update it from past and present threats. The paper presents certain authentication methods and security methods that are stronger than the existing methodologies, but regardless of how much security you bring to a cloud system there will be always be a point of vulnerability that can be used by hackers, this can only reduce by employing proper supervision or advanced AI systems, as far as the AI doesn’t go rogue. It is more better to have a world where everyone can work towards a united goal, by bringing in more global and communal awareness and a selfless work society we can hackers from causing harm and rather have them work for a better humanity on the technological side.

Abbreviations
PC – Personal Computer
HPC – High Performance Computing
AWS – Amazon Web Service
IT – Information Technology
Iaas – Infrastructure as a Service
Paas – Platform as a Service
Saas – Software as a Service
Faas – Function as a Service
IP – Internet Protocol
DNA – Deoxyribo Nucleic Acid

References
[1] H. R. Abdulshaheed, I. Al Barazanchi, H. T. Jaya, and D. Tunggal, “Smart Solutions Based-On Cloud Computing and Wireless Sensing,” Int. J. Adv. Sci. Technol., vol. 28, no. 8, pp. 526–542, 2019.
[2] C. Qiu, H. Yao, C. Jiang, S. Guo, and F. Xu, “Cloud Computing Assisted Blockchain-Enabled Internet of Things,” IEEE Transactions on Cloud Computing, pp. 1–1, 2019.
[3] G. Reese, “Cloud Application Architectures: Building Applications and Infrastructure in the cloud”, O'Reilly Media, 2009
G. Jia, G. Han, J. J. P. C. Rodrigues, J. Lloret, and W. Li, “Coordinate Memory Deduplication and Partition for Improving Performance in Cloud Computing,” IEEE Transactions on Cloud Computing, vol. 7, no. 2, pp. 357–368, Apr. 2019.

H. R. Abdulshaheed, S. A. Binti, and I. I. Sadiq, “Proposed a Smart Solutions Based-on Cloud Computing and Wireless Sensing,” Int. J. Pure Appl. Math., vol. 119, no. 18, pp. 427–449, 2018.

J. Narantuya, H. Zang, and H. Lim, “Service-Aware Cloud-to-Cloud Migration of Multiple Virtual Machines,” IEEE Access, vol. 6, pp. 76663–76672, 2018.

A. Garg and R. Rathi, “A Survey on Cloud Computing Risks and Remedies,” International Journal of Computer Applications, vol. 178, no. 29, pp. 35–37, Jul. 2019.

N. Venkateswaran, A. Shekhar, S. Changder, and N. C. Debnath, “Using machine learning for intelligent shard sizing on the cloud,” Period. Eng. Nat. Sci., vol. 7, no. 1, pp. 109–124, 2019.

S. Mahjabin, “Implementation of DoS and DDoS attacks on cloud servers,” Period. Eng. Nat. Sci., vol. 6, no. 2, pp. 148–158, 2018.

T. M. Mbelli, and B. Dwolatzky. “Cyber Security, a Threat to Cyber Banking in South Africa: An Approach to Network and Application Security”, Cyber Security and Cloud Computing (CSCloud), 2016 IEEE 3rd International Conference, IEEE, 2016, pp. 1-6.

T. S. Ruprah and A. S. Dange, “Enhanced Security in Cloud Using Data Partitioning Technique,” SSRN Electronic Journal, 2019.

S. Jaswal and M. Malhotra, “Identification of Various Privacy and Trust Issues in Cloud Computing Environment,” Cloud Security, pp. 992–1013, 2019.

I. Al-Barazanchi, Z. A. Jaaz, H. H. Abbas and H. R. Abdulshaheed, “Practical application of IOT and its implications on the existing software,” 2020 7th International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI), Yogyakarta, Indonesia, 2020, pp. 10-14, doi: 10.23919/EECSI50503.2020.9251302.

H. R. Abdulshaheed, S. A. Binti, and I. I. Sadiq, “A Review on Smart Solutions Based-On Cloud Computing and Wireless Sensing,” Int. J. Pure Appl. Math., vol. 119, no. 18, pp. 461–486, 2018.

I. Abdulshaheed, H. R., Yaseen, Z. T., Salman, A. M., & Al_Barazanchi, “An Evaluation study of WiMAX and WiFi on Vehicular Ad-Hoc Networks ( VANETs ),” IOP Conf. Ser. Mater. Sci. Eng. Pap., vol. 3, no. 12, pp. 1–7, 2020, doi: 10.1088/1757-899X/870/1/012122.

I. Al Barazanchi, H. R. Abdulshaheed, M. Safiah, and B. Sidek, “Innovative technologies of wireless sensor network : The applications of WBAN system and environment,” Sustain. Eng. Innov., vol. 1, no. 2, pp. 98–105, 2020.

H. R. Abdulshaheed, Z. T. Yaseen, and I. I. Al-barazanchi, “New approach for Big Data Analysis using Clustering Algorithms in Information,” Jour Adv Res. Dyn. Control Syst., vol. 2, no. 4, pp. 1194–1197, 2019.