International Journal of Engineering & Technology, 7 (3) (2018) 1161-1171

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i3.13075
Research paper

Literature review of security issues in saas for public cloud computing: a meta-analysis

Mohanaad Shakir [1] *, Maytham Hammood [2], Ahmed Kh. Muttar [3]

[1] Information Technology Department, Alburaimi University College (BUC), Oman
[2] College of Computer Science And Information Technology, University Tenaga National (Uniten), Malaysia
[3] Computer Science Dept., Tikrit University, Iraq
[4] Applied Science University, College of Administrative Sciences, Bahrain
**Corresponding author E-mail: mohanaad@buc.edu.om*

Abstract

Cloud computing is a rapidly growing technology due to its highly flexible uses and applications. It also has other features such as simplicity, quick data access and reduced data storage costs. Consequently, it has been widely used by many organizations. This widespread use of cloud computing among organizations causes many security issues. Moreover, cloud computing layers are likely to be jeopardized by many security risks such as privileged user access, data location, data segregation, and data recovery. This paper aims to prepare an ample debate of a literature review-based studies that provided important insights to researchers in the scope of security cloud computing. The researcher applied a relevant set of keywords. These keywords are limited to the title, abstract and keywords search archives published between 2010 and June 2017. The database search returned a total of 308 publications. In addition, we conducted backward-forward searches from the reference lists of relevant, quality previous works on the security framework in public cloud computing studies. Then, the researcher filtered the publications to only full text access articles that were written in English only. Finally, this study obtained a total of 53 publications. The findings of this paper address many important points such as authentication, data segregation, and encryption which are considered as the top concerns in security cloud computing. In addition, most of authentication layer is considered password as a prime criterion in determining authorizes user.

Keywords: *Cloud Computing; Security Issues in Cloud Computing; Authentication; Encryption; Saas; Security Framework in Cloud Computing; EPSB.*

1. Introduction

Cloud computing has rapidly grown through information technology as a result of its numerous services available for users[1]. Due to its various services available, there are a number of definitions that describe its functions and implementations. Cloud computing is defined as "a large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet"[2]. According to the National Institute of Standards and Technology (NIST), cloud computing is defined as "a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[3]. It is generally divided into three sections, namely deployment, service and characteristics[4], as shown in figure 1.

NIST defines cloud computing based on the four deployment models of public, private, hybrid and community[5]. Service models that NIST defines include Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)[6]. In addition, NIST has established a number of distinctive characteristics of cloud computing, including accessibility, on-demand self-services, elasticity, pay-as-you-go, versatility, share resources, security, reliability and performance. Overall, this paper presents the main security issues associated with cloud computing. In a related context, this paper shows the security issues in public cloud computing and literature review in security framework in cloud computing.

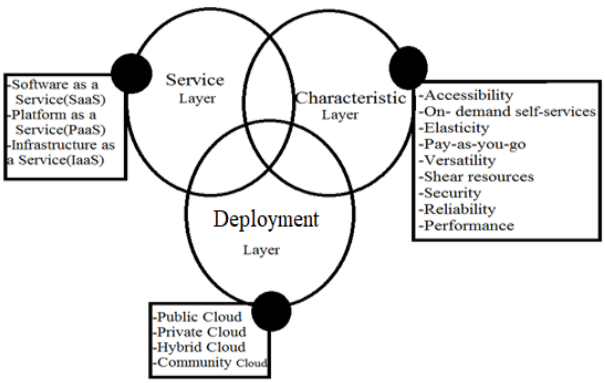


Fig. 1: Cloud Computing Layers.

2. Literature review

2.1. Security issues in public cloud computing

Gartner determined seven popular security issues that clients should tackle with vendors before a cloud computing system is

Copyright © 2018 Mohanaad Shakir et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

chosen. First is privileged user access, which has to do with the personnel who can maintain and access client data. Clients must ask Cloud Service Providers (CSPs) about their hiring practices and who is responsible for such processes[7]. Second is regulatory compliance. Regulatory compliance has to do with regular external audits and security certifications[8]. Third is data location. It is highly possible that your data may be processed and maintained in a different country, although you may not know it. In some countries, restrictions are applied to the overseas transfer of data[9]. In addition, virtualization technologies hinder the identification of the data location such that CSPs must follow local privacy requirements to safeguard the data. Fourth is data segregation. This stands for the division or categorization of data so that cloud clients can only access certain information without affecting that of others. CSPs should hire security to perform this, and data segregation should be performed by a hired security firm. Fifth is data recovery, which is important in terms of retrieving data in the case of calamities or unforeseeable circumstances. The CSP must be able to ensure that the storage media is reliable and that the data can be recovered to the fullest extent. Sixth is investigative support, which means having measures in place to monitor any illegal activity that may be occurring on the cloud. The last security risk is long-term viability. CSPs have the capability to make data available long-term or as long as necessary, even when companies are no longer in operation. Figure 2 below shows the security issues in cloud computing.



Fig. 2: Security Issues in Cloud Computing.

In addition, Carrol et al. [10]outline a number of concerns that are important in addressing cloud computing security issues. These concerns include administration and control, data security, network security, physical security, logical access, compliance and virtualization. Thus, any organization that uses cloud computing needs to manage the security issues and establish policies, rules and remedies for security vulnerabilities when storing sensitive data and sharing services with customers. CSPs should be able to provide security for data and applications to meet Service Level Agreements (SLAs)[11].

2.2. Security and privacy specifications in public cloud computing

Security deals with informational privacy, integrity, and availability, and is additionally characterised by Authorisation, Authentication, and Access control (AAA), as shown in Figure 2.



Fig. 3: AAA Triangle.

Privacy, in turn, relates to the adherence to certain legal and functional requirements, including client agreements, personal identification, and legit usage, as well as purpose constraints. Additional norms are control, compliance, and clarity. When these requirements are met, the cloud arrangement is considered to be lawfully operating. Below are some supplementary specifications according to ISO 7498- 2[12]:

i) Identification and authentication management applies to the functional checks for user identification and authentication that prevent antagonist malpractices within the cloud [13]. CSPs are therefore obliged to ensure valid client credentials are used when users are logging into their accounts. In most cases, this process of verification is achieved through a username–password system, adopted during the browser or cloud login stage. An optimal identification solution involves a two-factor authentication (2FA), which adds an additional verification step. However, such a solution poses some access limitations to the cloud services. Still, in order for client profiles to be safe and their information secure, authentication is an important part of the process.

ii) Authorization and access control deals with the fact that various users are entitled to different prerogatives when using cloud services, especially in the case of public clouds. Their privileges depend on the account type they have purchased from the CSP. It is crucial that the CSP rightfully administers users' permissions, privileges, and claims over acquired information. Additionally, elite members of the cloud should abide by certain internal regulations as well[14]. Unauthorized users should furthermore be prevented from abusing the information of legit customers. Google and Apple are among the companies that have tried to solve this issue by functional account segregation, meaning that staff members are always monitoring elite user activities and administrators with extended data access in order to prevent data abuse and hacker attacks. It is of utmost importance for client security for clients to completely trust in the CSP and vice versa; the same is valid for the client-administrator and CSP-administrator relationships [14].

iii) Confidentiality involves the numerous cloud access points and users, which makes it sensitive to illegitimate venues and pirate individuals. Clouds must ensure that only authorized users can access their data. Such precaution is especially mandatory for public clouds since they are most vulnerable. Software applications, shared information and profiles, information exposure, and weak user identifications are among the immediate threats concerning the cloud storage. The cloud's multitenancy characteristics pose the threat of user data abuse since resource sharing between clients can expose private information. This is largely due to the fact that a cloud separates its data assets only virtually. Information that has been deleted can be unlawfully retained and reconstructed because of the cloud's data remnants. Fraud protection should also be implemented because weak identification may result in illegitimate data access. It is mandatory that cloud service providers protect users from breaches coming from various software applications, which require access to the clients' information[15]. This data, although used by the application, must remain secure and unavailable to third parties. Privacy can be secured by popular techniques like 2FA [16] and encryption algorithms[17][18].

iv) Integrity is the cloud's attribute that deals with safeguarding cloud software from third-party unwanted actions like fabrication, theft, deletion, and alteration. It is associated with Atomicity, Consistency, Isolation, and Durability (ACID), which certifies data integrity. All four of these features must be ensured by the cloud service providers for all computing models. This can be done by avoiding illegal use of information and by using hash function algorithms[19]. The CSPs should focus not only on data but on network and hardware integrity as well.

v) Non-repudiation makes sure that the sender and recipient of a message cannot be confused, and thus cannot avoid taking responsibility for an action. Among the techniques that make this possible are timestamps, confirmation receipts, and digital signatures [19].
vi) Availability is the consistency of both hardware and software, which must also be at the user's disposal. There is no excuse for failure to provide these services on the CSP's end, even in situations regarding system errors, fraudulent activities, or breaches in security [15]. This is one of the key characteristics that make consumers prefer one cloud service provider to another. Other absolute fundamentals are minimum downtime, enterprise data security, Disaster Recovery (DR), and Business Continuity (BC)[20]. Availability depends on the use of replication techniques, recovery and backup devices and programs, and fault tolerance.
vii) Compliance and audit refers to the fact that legislative requirements must be strictly followed and the CSPs are obliged to act in accordance with local and international regulations concerning their field of operation[21]. Among the standards the CSPs should abide by are the Health Insurance Portability and Accountability Act (HIPAA), SAS 70, Payment Card Industry Data Security Standard (PCIDSS), and ISO [121]001 [31]. On the other hand, users also need to adhere to data encryption regulations when uploading, downloading, or transferring data using public networks and to the applications' software licenses. This often presents challenges to the CSPs because they are not able to constantly monitor the data that is being uploaded and cannot certify the actual compliance if it is requested by a client. Therefore, clients can also never be certain if they are acting lawfully because the CSPs cannot give them the relevant information regarding cloud procedures and common practices [22][9]. Therefore, it is crucial that the CSPs monitor and evaluate all activities at all times through a set of internal and external audit techniques. What the clients can be informed about are internal controlling techniques and processes and the results from any external audit report [20]. The biggest challenge before the auditors lies in the monstrous amount of data that needs to be supervised [13].
viii) Transparency pertains to the procedural clarity the CSPs must provide to their clients, who should be informed at all times about what is happening and what will happen to the information with which they operate. Users should also be aware of whom their cloud provider is and to what point his or her responsibility extends [21]. SLA is considered to be the means by which CSPs establish transparency as part of the client-provider relationship. The SLA is a legal obligation adopted by the cloud service providers and binds them to deliver the service the user has paid for, to keep track of all activities and report them in a professional way, to comply with all legal regulations, and to ensure maximum security for its clients.
ix) Governance refers to the CSP's obligation to protect user information from any external intruder with harmful intentions. This is a rather challenging responsibility since the data is processed and kept at a remote distance, which opens it to attacks. More often than not, clients are aware of this threat and require information about who has requested access to their transfers. Virtualization and sharing of resources pose additional risks in terms of security[23]. CSPs should govern the clouds with respect to these hazards by applying various fraud monitoring procedures and policies [21].
x) Accountability refers to the CSPs being held responsible for implementing the correct security mechanisms and reacting timely in case of malware or hacks [21].

3. Method

This section presents the security issues in cloud computing, the authentication model, and the different types of security frameworks that have been proposed. This study covered 50 papers from IEEE, ProQuest, ScienceDirect, Scopus and the Springer database, which are related to the research scope, as shown in figure 4.

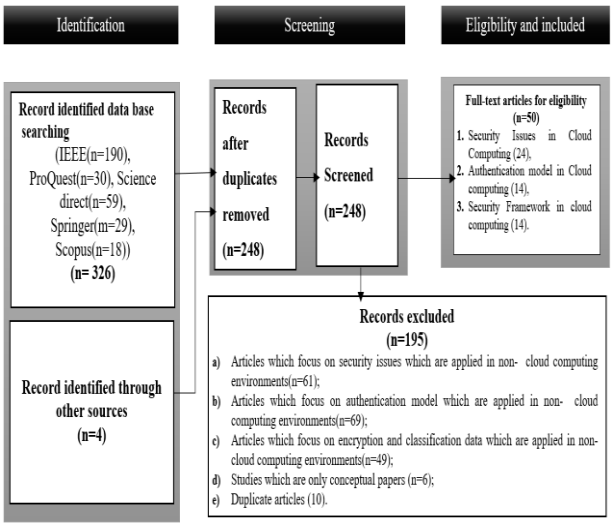


Fig. 4: Selection Process of Articles Extraction.

3.1. Data sources and search strategies

A researcher performed automatic searches using the search engines of the IEEE, ProQuest, Science Direct, and Springer electronic databases. The researcher applied a relevant set of keywords and phrases such as 'Authentication Model,' 'cloud computing Security,'' Security Requirement,' 'Security Framework in cloud computing,' 'Encryption Algorithm in cloud computing,'' Data Classification,'' Security Issues in cloud computing,' and 'cloud computing Security Processes.' These keyword searches are limited to the title, abstract and keywords search archives published between 2010 and June 2017. The database search returned a total of 308 publications. In addition, we conducted backward-forward searches from the reference lists of relevant, quality previous works on the security framework in public cloud computing studies. Then, the researcher filtered the publications to only full text access articles that were written in English only. Finally, this study obtained a total of 53 publications.

3.2. Inclusion/exclusion criteria

The researcher narrowed down the full text publication based on the Inclusion and Exclusion criteria. Inclusion criteria consists of articles that present the Authentication Model related to and within cloud computing firms, articles that included or mentioned their research approach and articles that proposed and evaluated research models or frameworks. Meanwhile, Exclusion criteria consists of articles which focus on security issues, authentication models, and the encryption and classification of in non-cloud computing environments, studies that are only conceptual papers and duplicate articles. Table 1 shows the Inclusion and Exclusion criteria used in this study.

Table 1: Inclusion and Exclusion Criteria

Inclusion criteria	Exclusion criteria
a) Articles related to Security framework in cloud computing implementation written in English.	a) Articles which focus on security issues which are applied in non- cloud computing environments.
b) Articles which are related to Authentication	b) Articles which focus on authentication model which are

	Model implementation within cloud computing firms		applied in non- cloud computing environments.
c)	Articles which are related to encryption and classification data implementation within cloud computing firms	c)	Articles which focus on encryption and classification data which are applied in non- cloud computing environments.
d)	Articles which included their research approach	d)	Studies which are only conceptual papers
e)	Articles which proposed and evaluated research frameworks	e)	Duplicate articles

Finally, the researcher obtained a total of 53 relevant studies for this literature analysis. The literature analysis is based on full text reading and documentation presented in this paper. The analysis of each paper is followed by three main topics, including security issues, the Authentication model, and the security framework related to the research problems.

4. Results

Of the 52 studies published on cloud computing security from 2010 to 2017, frequency of publication focused on security issues in cloud computing and develop authentication layer in cloud computing. Below I detail the results of our meta-analysis based on three research question.

4.1. Research question 1

Major Research Purposes, Online Database, and Papers Citation

4.1.1. Distribution of research purposes

Author classified each paper into one of three categories according to the research purpose: (1) Security Issues in Cloud Computing (24 papers), (2) Authentication models in Cloud Computing (14 papers), and (3) Security Framework in Cloud Computing (14 papers), As seen in Fig. 5, evaluating the) Security Issues in Cloud Computing was the most common research purpose (46.153%), followed by Authentication models in Cloud Computing (26.923%) and Security Framework in Cloud Computing (26.923%).

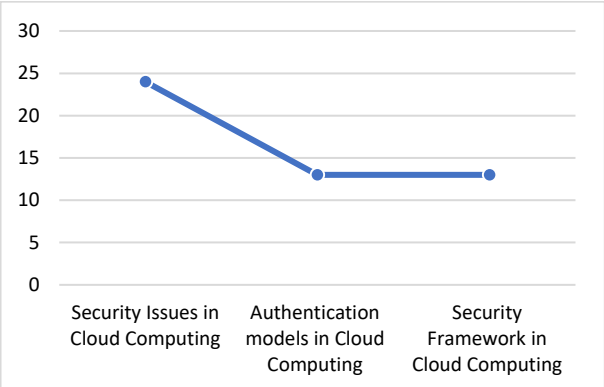


Fig. 5: Distribution of Papers Based on Categories.

4.1.2. Distribution of online database

This section presents the distributions of papers based on online database. Those pertaining to the percentage of IEEE was (48%). The ACM has the percentage (10%). The Science Direct , Prequest and others have the same percentage (8%). The percentage of SCOPUS was (14%). Additionally, The Springer percentage was (4%).

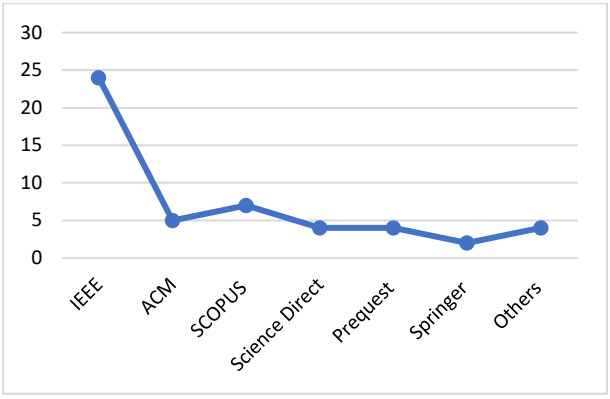


Fig. 6: Distribution of Papers Based on Online Database.

4.1.3. Distribution of papers citations

As seen in figure 7 papers have been distributed based on the number of citation in the search engines of the IEEE, and in figure 8 papers have been distributed based on the number of citation in the others search engines. The main purpose of this analysis to determine the dependability level of researchers on these papers. The analysis results are appearing the 80% from these papers got up to 190 citations. Therefore, these papers have a high accreditation in scientific researchers' range. Thus, these papers are considering in this article.

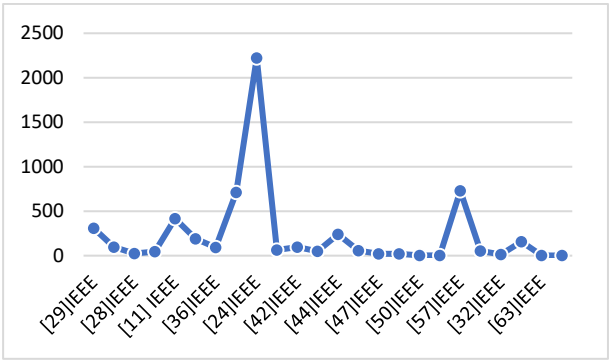


Fig. 7: Number of Citation in the Search Engines of the IEEE.

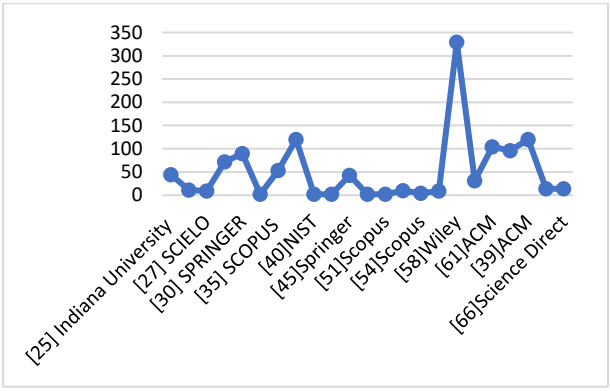


Fig. 8: Number of Citation in Others Search Engines.

4.2. Research question 2

Security Issues in Public Cloud Computing, Scope of security and privacy specifications in public cloud computing and security mechanisms

4.2.1. Distribution based on security issues in public cloud computing

this section presents the distributions of papers based on the purposes of security issues in public cloud computing. Those pertaining to the percentage of privileged was (40%). The regulatory

compliance, data segregation and data location have the same percentage (13%). The percentage of data recovery was (14%). Additionally, (7%) was the percentage for the investigative long-term viability, as seen in Fig. 9.

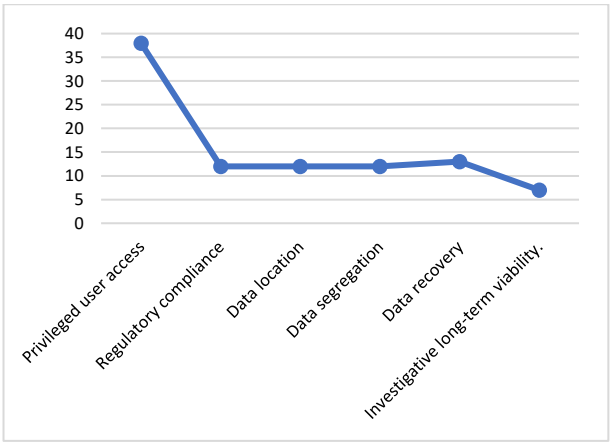


Fig. 9: Distribution of Papers Based on Security Issues in Public Cloud Computing.

4.2.2. Distribution based on security mechanism

This section presents the distribution of studies based on security mechanism. The main purpose of this analysis is to determine the most common security mechanism had been applied from researchers in cloud computing security. Fig. 7 indicates encryption and just review paper most frequently on security mechanism (26%), followed by certificate authority(CA) (12%), watermark and risk management (8%), firewall, and SSL (4%) and PKI, digital signature, information hiding, kerberos, proxy and intrusion detection (2%)" see Figure 10".

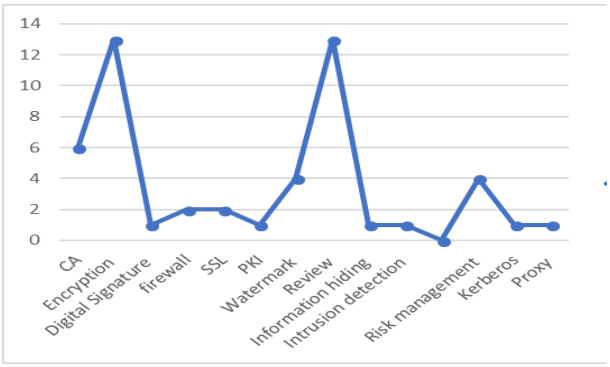


Fig. 10: Distribution of Papers Based on Security Mechanism.

4.2.3. Distribution based on Scope of security and privacy specifications in public cloud computing

This section presents the distribution of studies based on Scope of security and privacy specifications in public cloud computing. The main aim of this analysis is to determine the most common research scope had been applied from researchers in security and privacy specifications in public cloud computing Fig. 8 In terms of Authorization and access control and Confidentiality were the most common focus (19%), followed by Identification and authentication management (18%), Availability (12%), Integrity (9%), Accountability (7%), Compliance and audit (5%), Non-repudiation and Governance (4%) and Transparency (3%).

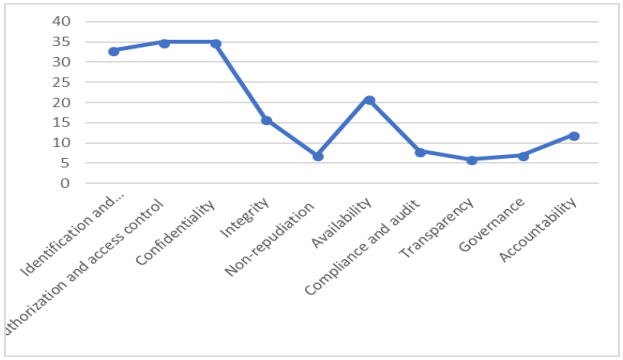


Fig. 11: Papers Distribution Based on Scope of Security and Privacy Specifications in Public Cloud Computing.

4.3. Research question 3: papers objectives, a suggested solution, and paper results

4.3.1. Papers objectives, a suggested solution, and paper results in authentication in public cloud range

This section presents the distributions of papers based on the purposes of main papers categories such as Objectives, Aspect of authentication model and papers results, shown in table 1 below. Generally, Authentication layer has two important activates, user Identification and access. The aim of this analysis to insurance the literature review about the aspects of authentication layer which has been proposed from scientific researchers whose interested in cloud computing security, as shown as in table 2 below.

Table 2: Papers Distribution Based on Papers Objectives, a Suggested Solution, and Paper Results in Authentication in Public Cloud Range

Articles and publisher	Objectives	Aspect of authentication model	Articles Results
[24] [25] IEEE	To suggest a cloud security trust model and certain social security	sub-classified into three core groups – multiple stakeholders, open space, and handling of critical information issues	The trust model in this paper blocks any malicious access into the cloud computing environment. The current firewall software and trust models are evaluated in [25]
[26] IEEE	To determine the best approach to avoid any fraudulent flows	Transport Layer Security (TLS) should be used for the communications between switches and control planes	This study recommended using a middle box approach where traffic from the control plane should be directed and a dynamic security policy should be enforced on all flows to avoid any fraudulent flows proposed mechanism is comparing the security authorization of providers of new rules with the conflicting rule providers and make a decision whether to pass such a flow or not.
[27] Springer	To proposed mechanisms to prevent unauthorized access	The deployment model, identity and access management, security zones, FWs, hypervisor introspection and must be applied, and regarding DoS attacks, virtual load balancers and virtual Domain Name System (DNS) servers should be utilized.	Recommends security mechanisms including hypervisor introspection and centralized security management for NFV deployment. A secure key storage should be provided using specialized Hardware Security Models (HSM) so it is not accessible and visible by third-party virtual Network Functions (vNF).
[28] IEEE	To proposed trust model has ability to enhancing	Supplementary security framework	Suggests relevant solutions to already existing issues concerning both cloud providers and users.

	the standard security.		
[29] IEEE	To pinpointed security SaaS concerns	The fact that cloud data can be accessed via any installed software	This software can be settled through a mechanism separating the software from the users and the data provided by the coordinator, software, or data provider
[30] IEEE	To examine the secure connectivity in cloud computing by reviewing existing network security technologies	Introduce CaaS model (inter- and intra-cloud communication) B2B	The researcher presents a safe communication architecture where B2B is involved through a CaaS model (inter- and intra-cloud communication) and and presenting an electronic contract-based solution that provides a secure Connectivity as a Service (CaaS).
[31] ITU	To proposed authentication model for hybrid cloud computing	That model operates through PKI and a CA system with single data encryption and comprises three main elements	The first element is a CA model in which the public cloud issues a secret ID to a private cloud; the CA, in turn, examines the validity of both IDs and approves access only in case of a match. The second element is the public cloud, which sends the secret ID notice to the private cloud. Respectively, the third element is the private cloud, which requests and receives the secret ID. For avoiding unauthorized access.
[32] IEEE	To avoid any illegal access to the documents	Secure Authentication Model (SAM)	implemented using a wireless body area network and runs using a high-power, efficiency-based. The researcher proposed security system for WBAN with low computational complexity for the secure transaction
[33] Scopus	To avoid any illegal access to the documents	electronic personal synthesis behavior(EPSB)	Raising the rate of avoid an unauthorized access
[34] Scopus	To protect the system from both inside and outside attacks	USBs and Smart Cards	The researcher suggested the model for hiding authentication on public cloud
[34] [35] Scopus	To determine when an outside user attempts to login using a proxy gateway and interface	VM interface	Avoid unauthorized access
[36] IEEE	To protect information in the cloud from leaking	follow the authentication and confidentiality approach	It assesses any privacy leak risks and, if the operation is deemed safe. The risk itself is evaluated through the employment of another model specifically designed to prevent privacy leaks.
[37] IJARET	To propose a multi-authority model based on user behavior	Introduce a multi-authority model. , it is subdivided into two models – system and security one. The former is associated with five entity types: owners (data owners), users (data consumers), AAs (attribute authorities), CA (certificate authority), and server (the cloud server).	A multi-partite graph-based authentication model was presented later that deals with trust and security issues at the user level.
[38] IEEE	To Propose trust model	Trusted Support Service (TSS)	a cloud computing system built upon a dependable platform and a prototype for Trusted Support Service (TSS) was presented. The two systems were combined to work together to identify fraudulent users.

4.3.1. Papers objectives, a suggested solution, and paper results in security issues in public cloud range

This section presents the mains security issues in public cloud computing has been concerned from researchers. In this part, I classified all papers based on three sectors: (1) objectives, (2) A suggested solution and (3) Articles Results. The output of this analysis provides a full perspective about security issues and what is the solutions has been suggested to avoid these issues and what is the results"see table 3 below".

Table 3: Distribution Papers Based on Objectives, A Suggested Solution, and Paper Results in Security Issues in Public Cloud Range

Articles and publisher	Objectives	Aspect of authentication model	Articles Results
[39] IEEE	To Prevent Any Fraudulent Operations	1. Authentication. 2. Data Integration. 3. Data Encryption. 4. User protection.	Increase Platform Security by: 1. the information must be safeguarded through processes like detection, block modification, and insertion; 2. stressed that cloud computing must be used in such a way as to ensure that the data is both safe and secure.
[40] Indiana Un.	1. To Ensure the Cloud's Optimal Security 2. To Diagnose Privacy Risks	Effective Privacy Protection Scheme (EPPS) (employs encryption algorithms to diagnose privacy risks)	Increase Cloud Security By 35–50%.

[22] IEEE			To enhance cloud computing security	(The Application of Homomorphic Encryption Algorithm) The concept of (Mobile Device Search Scheme; And Secure Cloud Storage was introduced	It addresses SMS storage issues by encrypting the texts and transferring them to the cloud. After that, it sends them back to the mobile device and, in this way, stores and protects them.
[41] CNKI			To find viable solutions to pending threats and improve the overall safety of the cloud performance	Security Issues Can Be Addressed Effectively Through System Data Analysis and Cloud Computing	We need A number of security actions and methods must be applied to minimising exposure to hacker attacks on the cloud level and allowing for data to stay within its designated boundaries without leaking out
[42] SCIELO			To enhance data security in cloud computing (data privacy)	It comprised of three major elements – prediction, generation of data, and information marking.	The model masks valuable data so that it cannot be linked to the mark. The potential user of the data should then apply a secret key in order to get to it.
[43] IEEE			To integrity evaluation technique was discussed. Cloud safety issues were again listed and elaborated on.	All valuable data must be encrypted when using cloud storage	Data exposure to corruption, theft, and plagiarism, which in turn presents a problem on confidence level because its remote storage.
[23], [44], Springer [45]IEEE			To explain data integrity in details and the importance of its maintenance To protect all dynamic processes pertaining to the outsourced data, including appending, block modification, and deletion on the basis of a particular security analysis.	. The authors have developed a unique framework for maintaining cloud security. It involves active cooperation between the service and cloud providers and the end users	When supported properly, it can prevent hacker attacks, malignant data infusion, Byzantine failure, and server colluding intrusions. Through cloud security adjustment
[22] IEEE	To identifies possible security issues in cloud computing and determine the necessary security features and possible solutions	The identified problem types are access, cloud infrastructure, data, and compliance	Several steps for maintaining data security must be taken, including standardising industry farms' safety processes, performing regular analysis of user behaviour to identify possible threats in a timely manner, and emphasised data confidentiality, user responsibility to adhere to regulatory standards, and identification of probable hazards.		
[11] IEEE	To determine security guideline for cloud computing	Proposed security guideline for cloud computing	A guideline that includes cloud transparency, cloud governance, and cloud computing effects for managing the security of the cloud		
[46] IEEE	To determine risk management for problems regarding cloud computing security	Proposed four points for specific vulnerability were included	Four points that could be applied for specific vulnerability were included. These points are as follows: 1) it is prevalent or intrinsic in cloud computing core technology; 2) one of NIST's essential cloud characteristics is evident in its roots; 3) it is formed by cloud innovations that lead to hard implementation of security controls; and 4) the authors were sure that more cloud-specific vulnerabilities need to be identified as an important aspect of cloud computing security		
[47] SCOPUS	To diagnosis security problems in cloud computing	Prepared preliminary study	The organizations or institutions are very concerned in improving the security of cloud computing through the application of the authority model and dynamic classification of data model based on the multi-level security. They prefer to develop the multi-key cipher algorithm in order to manage the encryption based on the level of security. Based on the results of this study, it is recommended that organizations must apply new policies in classifying the data into many security levels based on the nature of data to save time, and effort.		
[48]	To understand risk	1. Provided a mapping	Risk management in cloud computing can be divided into three levels: level		

SCOPUS , ISI	management for problems regarding cloud computing security	scheme for security risks; 2. Attempted to develop approaches to address such issues	1 is for major divisions (risks for companies introducing cloud computing, risks for cloud service provider, and others), level 2 is for the middle division (operation, system, and facility), and level 3 is for several recorded risks based on cloud security problems (risk transference, risk acceptance, risk avoidance, and risk mitigation).
[49]IEEE [50],IEEE [51]IEEE [52]IEEE	To address security and privacy concerns in cloud computing	Researchers put forward four methods to address security and privacy concerns	Four methods to address security and privacy concerns in cloud computing, namely access control, policy integration, identity management, and user control of their data
[53] ACM	To study security policies, hardware security, and software security in cloud computing	Proposed a method to address security and privacy	The use of open standards to address such concerns as vendor lock-in and incompatibility
[54] NIST [55] SCOPUS	To determine the cloud computing security standards	Proposed cloud computing security standards that may apply in cloud computing	NIST has determined the policies, roles, and responsibilities such as planning, ensure and accreditation as the main points that must be included in any security plan in cloud computing

4.3.2. Papers objectives, a suggested solution, and paper results in security framework in public cloud range

This section presents the results of papers in security framework with public cloud computing which has been proposed from researchers. In this part,

I classified all papers based on three sectors: (1) objectives, (2 Security Framework Layers and (3) papers Results. The output of this analysis provides a full perspective about security framework layers and what is the solutions has been suggested to avoid these issues and what is the results.

Table 4: Distribution Papers Based on Objectives, A Suggested Solution, and Papers Results in Security Framework in Public Cloud Range

Articles and publisher	Objectives	Security Framework Layers	Papers results
[57] Wiley	To achieve better overall Quality of Service (QoS), reliability and cost efficiency by utilizing multiple clouds	Three authentication level" 1. The first level requires a legitimate certificate 2. The second and third steps involve certificate validity checks and appointing the user to a specific server that they are authorised to use	The authors further proposed a coRBAC cloud authentication model, which supplies the user with three authentication levels upon login
[58] Accent	To improve security framework for cloud computing via web	1. Authentication layer; 2. Encryption layer; 3. Privacy Protection	This model allows for better security, as the user has full control when accessing the cloud
[59] IEEE	to determine intricate security features in cloud computing	1. Data management	This new security solution is fully fit for the processing and retrieval of the encrypted data, and effectively leading to the broad applicable prospect, the security of data transmission and the storage of the cloud computing
[60] ACM	To improve framework to avoid any attack	1. Authentication layer; 2. Access control; 3. Encryption layer	Suggest behavioural authentication in contrast to traditional authentication with credentials, certificate or key based authentication
[61] IEEE	To pointed out as a possible answer to the cloud computing dependability dilemma	1. Authentication layer; 2. Management layer.	This paper proposes a conceptual SLA framework for cloud computing to support dependability by using a trust management model in the process of selecting the cloud providers. And to determine a reliable method for selecting the most secure providers of cloud resources.
[22] Elsevier (Science Direct)	To develop security framework for business to protect cloud computing from Viruses and trojan attack	1. Authentication layer; 2. Intrusion detection; 3. Encryption layer.	Proposed security framework for business cloud computing based on blending of multilayered security with policy, real services, and business activities have been showed
[53] ACM	To develop security system for enforcing security in cloud computing	1. Authentication layer	Proposed collaborative computing systems under name UBSF. The decision of UBSF is made based on objects, subjects, authorization, conditions, and obligations. Sensors, policy decision point (PDP), directory service, and usage monitor (UM) are considered a core of authorization architecture
[62] IEEE	To improve accountability in cloud computing	1. System layer; 2. Data layer; 3. Workflow layer.	Proposed a Trust cloud framework. This framework is considered a theoretical framework because it didn't cover computational demonstrations, case studies, and quantitative analyses.

[63] IEEE	To avoid failure of any single cloud, encrypt user files.	1. 2.	Authentication layer; Encryption layer.	Proposed security framework for cloud computing. The experimental results show that, the time cost of the Shamir's secret partitioning process and symmetric encryption process almost can be negligible when the key size is as long as 386 bytes, and the proxy re-encryption process takes about 1.6 seconds in average
[64] IEEE	To keep track of the genuine usage of end-user's information in the cloud	Authentication layer		proposed data logging framework performs correctly as expected and shows potential to improve cloud security. According to the experimental results, the proposed framework may help decrease unauthorized access, data theft, and data loss
[65] Elsevier (Science Direct)	To protect storing data in cloud computing	Encryption layer		Proposed a homomorphic encryption of data in cloud computing
[66]Elsevier (Science Direct)	To review Symmetric and Asymmetric algorithms with emphasis on Symmetric Algorithms	Encryption layer		Presented a brief overview and comparison of Cryptographic algorithms

4.4. Research question 4: what common layers are using in security framework in public cloud?

As seen in figure 12 papers have been distributed based on the security framework in cloud computing. The authentication layer was the most common research purpose with a percentage of (35.29), followed by integrating of data (29.41%), encryption layer (23.52%), system layer (5.89%), and workflow layer (5.89%).

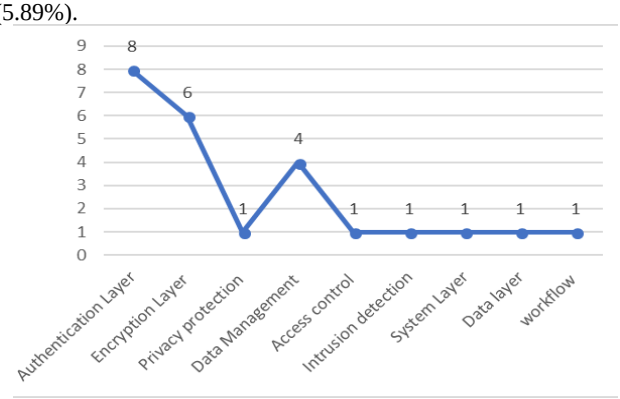


Fig. 12: Papers Distribution Based on Scope of Security and Privacy Specifications in Public Cloud Computing.

4.5. Research question 4: can conclude new research gap from these papers?

Authentication, encryption, and data integration were the top research topics in cloud computing [64]. Authentication is considered as one of the key issues in cloud computing since it is engaged with the functional checks for user identification and authentication that prevent antagonistic attacks within the cloud [13]. In the same sense, authorization and access control deals with the fact that various users are entitled to different prerogatives when using cloud services, especially in the case of public clouds. Their privileges depend on the account type they have purchased from the CSP [14]. Several scholars proposed various types of authorization models in cloud computing. These models have internally applied a set of security techniques such as SSL, Key management, Digital signature, and others. However, all these models do not address the following points:

1) Most of the authorization models considered the password as a primary criterion in determining the authorized user regardless of who entered the password (original user or other).
2) Inadequate concentration on both the record and analysis of the behavior of the authorized user.

Data encryption shifts the data from a readable style to an unreadable style by using an encryption algorithm[68]. The purpose of data encryption is to protect the confidentiality of digital data, which is stored on computer systems and transmitted using the Internet or another computer network [66]. Moreover, storing data as a cipher text prevents the exposure of information to change, theft, damage, or copying and affects the level of confidence in the information [65]. Furthermore, multiple types of encryption models proposed by cloud computing scholars have led to a set of security techniques, including RSA, RC4, DES, and others, these models did not address the following points.

1) They did not automatically encrypt data in a way that is commensurate with the level of data importance.
2) They did not link the security classification of data with encryption.

5. Conclusion

Cloud computing is a multi-layer data storage model that has been extensively and widely applied in information technology. It is generally divided into three layers, including the deployment layer, service layer and characteristics layer[3]. Its full scalability, reliability and high performance have made it indispensable for the achievement of organizational objectives [1, 2]. The security issues, such as authentication, access control, and data segregation, are the top concerns in cloud computing [3]. Moreover, cloud computing layers are likely to be jeopardized by many security risks such as privileged user access, data location, data segregation, and data recovery[66][67]. The public type of cloud computing is one of the deployment layers that can be accessed by public users through the Internet [8]. In a related context, SaaS (Software as a Service) is a type of service layer that can be used as a point of access for data stored in the public cloud [9]. SaaS can be accessed by potential users through a website or program interface through applying password, at anytime from anywhere and by using any device, as it works on registering and giving all users authorized access [67].

Many famous organizations such as iCloud suffer from password leaks in authentication layer which can be achieved through widespread methods such as intrusions, impersonations, Man In The Middle Attacks (MITMA) and spoofing [67][20]. This problem leads to the release of customer information as well as other losses, namely: financial loss and loss of privacy[67]. These potential security problems offer any potential intruder the opportunity to obtain an authorization password to access data storage. An intruder, who accesses the public cloud through an authorized password, device, or network on the first attempt, will have the authority of the original users to access data saved in cloud computing, as shown in figure 13. Therefore, organizations need an algorithm which is able to effectively detect these illegal breaches. Thus, this paper is determining two major security problems, where the main problem lies in the diagnosis of unauthorized users in some critical cases, such as when the unauthorized user has the original password by illegal methods. As for the other problem, it is the mech-

anism of dynamically classifying and encrypting data based on the security level of the data before being saved in the cloud.

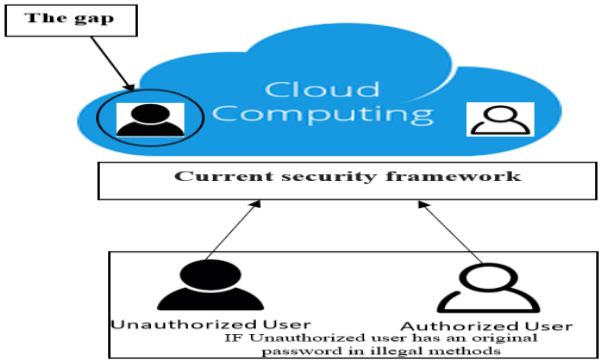


Fig. 13: Research Gap.

With regards to the Main problem, there is no algorithm to diagnose unauthorized users when they try to log on to a cloud through an authorized password, device, and network on the first attempt. Therefore, the original user's authority will grant unauthorized users access to possibly all data in the cloud. In the other problem, the organizations or institutions are very concerned with improving the security of cloud computing through the application of the authority layer and dynamic classification of data layer based on multi-level security [47]. However, there is no standard model that has the potential to determine the best and most accurate classification and encryption methods of data based on data authority and security levels. Hence, the current study designs a security framework to improve the security processes of SaaS in public cloud computing to address these problems.

Acknowledgements

We thank the colleagues who provided significant input to the research presented in this paper, in particular Mohamad Yahya Abdullah, Instructor at Alburaimi University College, as well as Sami Abdullah who helped with the corrections in the English language.

References

[1] M. M. Boroujerdi and S. Nazem, "Cloud computing: changing cogitation about computing," World Acad. Sci. Eng. Technol., vol. 58, pp. 1112–1116, 2009.
[2] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," in Grid Computing Environments Workshop, 2008. GCE'08, 2008, pp. 1–10. https://doi.org/10.1109/GCE.2008.4738445.
[3] V. Kundra, "Federal cloud computing strategy," 2011.
[4] P. Mell, T. Grance, and others, "The NIST definition of cloud computing," 2011.
[5] P. Jadhwani, J. Mackinnon, and M. Elrefal, "Cloud Computing Building a Framework for Successful Transition," GTSI, North. Virginia, 2009.
[6] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Comput. Commun. Rev., vol. 39, no. 1, pp. 50–55, 2008. https://doi.org/10.1145/1496091.1496100.
[7] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "TrustCloud: A framework for accountability and trust in cloud computing," in Services (SERVICES), 2011 IEEE World Congress on, 2011, pp. 584–588. https://doi.org/10.1109/SERVICES.2011.91.
[8] F. Sabahi, "Cloud computing security threats and responses," in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, 2011, pp. 245–249. https://doi.org/10.1109/ICCSN.2011.6014715.
[9] D. Teneyuca, "Internet cloud security: The illusion of inclusion," Inf. Secur. Tech. Rep., vol. 16, no. 3, pp. 102–107, 2011. https://doi.org/10.1016/j.istr.2011.08.005.
[10] M. Carroll, A. Van Der Merwe, and P. Kotze, "Secure cloud computing: Benefits, risks and controls," in Information Security South Africa (ISSA), 2011, 2011, pp. 1–9.
[11] K. Popović and Ž. Hocenski, "Cloud computing security issues and challenges," in MIPRO, 2010 proceedings of the 33rd international convention, 2010, pp. 344–349.
[12] S. D. Castilho, E. P. Godoy, T. W. L. Castilho, and F. Salmen, "Proposed model to implement high-level Information Security in Internet of Things," in Fog and Mobile Edge Computing (FMEC), 2017 Second International Conference on, 2017, pp. 165–170.
[13] Z. Wang, "Security and privacy issues within the Cloud Computing," in Computational and Information Sciences (ICCIS), 2011 International Conference on, 2011, pp. 175–178. https://doi.org/10.1109/ICCIS.2011.247.
[14] E. Mathisen, "Security challenges and solutions in cloud computing," in Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on, 2011, pp. 208–212. https://doi.org/10.1109/DEST.2011.5936627.
[15] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Futur. Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, 2012. https://doi.org/10.1016/j.future.2010.12.006.
[16] D. Abraham, "Why 2FA in the cloud?," Netw. Secur., vol. 2009, no. 9, pp. 4–5, 2009. https://doi.org/10.1016/S1353-4858(09)70097-2.
[17] F. Scott, M. Itsik, and S. Adi, "Weakness in the key scheduling algorithm of RC4," in Proceedings of the 8 Annual Workshop on SAC, 2001.
[18] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in cloud computing," in Information Security for South Africa (ISSA), 2010, 2010, pp. 1–7.
[19] A. Youssef and M. Alaqeel, "Security Issues in Cloud Computing.," GSTF J. Comput., vol. 1, no. 3, 2011.
[20] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011. https://doi.org/10.1016/j.jnca.2010.07.006.
[21] E. C. Amazon, "Amazon elastic compute cloud (Amazon EC2)," Amaz. Elastic Comput. Cloud (Amazon EC2), 2010.
[22] A. Tripathi and A. Mishra, "Cloud computing security considerations," in Signal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference on, 2011, pp. 1–5. https://doi.org/10.1109/ICSPCC.2011.6061557.
[23] A. E. Youssef, "Exploring cloud computing services and applications," J. Emerg. Trends Comput. Inf. Sci., vol. 3, no. 6, pp. 838–847, 2012.
[24] H. Sato, A. Kanai, and S. Tanimoto, "A cloud trust model in a security aware cloud," in Applications and the Internet (SAINT), 2010 10th IEEE/IPSJ International Symposium on, 2010, pp. 121–124. https://doi.org/10.1109/SAINT.2010.13.
[25] Z. Yang, L. Qiao, C. Liu, C. Yang, and G. Wan, "A collaborative trust model of firewall-through based on Cloud Computing," in Computer Supported Cooperative Work in Design (CSCWD), 2010 14th International Conference on, 2010, pp. 329–334. https://doi.org/10.1109/CSCWD.2010.5471954.
[26] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," in Future Networks and Services (SDN4FNS), 2013 IEEE SDN For, 2013, pp. 1–7.
[27] P. Schoo, V. Fusenig, V. Souza, M. Melo, P. Murray, H. Debar, H. Medhioub, and D. Zeghlache, "Challenges for Cloud Networking Security," in MONAMI, 2010, pp. 298–313.
[28] W. Li, L. Ping, and X. Pan, "Use trust management module to achieve effective security mechanisms in cloud environment," in Electronics and Information Engineering (ICEIE), 2010 International Conference On, 2010, vol. 1, pp. V1--14. https://doi.org/10.1109/ICEIE.2010.5559829.
[29] Z. Song, J. Molina, and C. Strong, "Trusted anonymous execution: A model to raise trust in cloud," in Grid and Cooperative Computing (GCC), 2010 9th International Conference on, 2010, pp. 133–138. https://doi.org/10.1109/GCC.2010.37.
[30] S. Chen, S. Nepal, and R. Liu, "Secure connectivity for intra-cloud and inter-cloud communication," in Parallel Processing Workshops (ICPPW), 2011 40th International Conference on, 2011, pp. 154–159.
[31] X. Recommendation, "509-The Directory: Public-key and attribute certificate frameworks," Int. Telecommun. Union, 2000.
[32] S. Sridharan and G. R. Kiran, "Secure authentication model for online health monitoring system," in Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on, 2013, pp. 1–5. https://doi.org/10.1109/ICCCNT.2013.6726758.

[33] M. Shakir, A. B. Abubakar, Y. Yousoff, M. Al-Emran, and M. Hammood, "APPLICATION OF CONFIDENCE RANGE ALGORITHM IN RECOGNIZING USER BEHAVIOR THROUGH EPSB IN CLOUD COMPUTING," J. Theor. Appl. Inf. Technol., vol. 94, no. 2, p. 416, 2016.

[34] L. F. B. Soares, D. A. B. Fernandes, M. M. Freire, and P. R. M. Inácio, "Secure user authentication in cloud computing management interfaces," in Performance Computing and Communications Conference (IPCCC), 2013 IEEE 32nd International, 2013, pp. 1–2. https://doi.org/10.1109/PCCC.2013.6742763.

[35] I. Singh, "Secc: Authentication and Access Control Mechanism for Secure Cloud Networks and Services," Birla Institute of Technology Mesra, 2015.

[36] M. Farhatullah, "ALP: An authentication and leak prediction model for Cloud Computing privacy," in Advance Computing Conference (IACC), 2013 IEEE 3rd International, 2013, pp. 48–51. https://doi.org/10.1109/IAdCC.2013.6514192.

[37] K. Kaur and S. Vashisht, "Data Separation Issues in Cloud Computing," Int. J. Adv. Res. Eng. Technol., vol. 1, no. X, pp. 26–29, 2013.

[38] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," IEEE Trans. Serv. Comput., vol. 5, no. 2, pp. 220–232, 2012. https://doi.org/10.1109/TSC.2011.24.

[39] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Trans. parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, 2011. https://doi.org/10.1109/TPDS.2010.183.

[40] S. Srinivasamurthy and D. Q. Liu, "Survey on Cloud Computing Security--Technical Report," Dep. Comput. Sci. Indiana Univ. Purdue Univ. Fort Wayne, 2010.

[41] W. Liu, "Research on cloud computing security problem and strategy," in Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, 2012, pp. 1216–1219.

[42] M. C. Liberatori and J. C. Bonadero, "AES-128 cipher: Minimum area, low cost FPGA implementation," Lat. Am. Appl. Res., vol. 37, no. 1, pp. 71–77, 2007.

[43] R. Chalse, A. Selokar, and A. Katara, "A new technique of data integrity for analysis of the cloud computing security," in Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on, 2013, pp. 469–473. https://doi.org/10.1109/CICN.2013.103.

[44] C. Cid, S. Murphy, and M. Robshaw, Algebraic aspects of the advanced encryption standard. Springer Science & Business Media, 2006.

[45] C. Basescu, A. Carpen-Amarie, C. Leordeanu, A. Costan, and G. Antoniu, "Managing data access on clouds: A generic framework for enforcing security policies," in Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on, 2011, pp. 459–466. https://doi.org/10.1109/AINA.2011.61.

[46] M. Almorsy, J. Grundy, and A. S. Ibrahim, "Collaboration-based cloud computing security management framework," in Cloud Computing (CLOUD), 2011 IEEE International Conference on, 2011, pp. 364–371.

[47] M. Shakir, A. B. Abubakar, Y. Bin Yousoff, A. M. Sagher, and H. Alkayali, "DIAGNOSIS SECURITY PROBLEMS IN CLOUD COMPUTING FOR BUSINESS CLOUD," J. Theor. Appl. Inf. Technol., vol. 90, no. 2, p. 151, 2016.

[48] N. Robinson, L. Valeri, J. Cave, T. Starkey, H. Graux, S. Creese, and P. P. Hopkins, "The cloud: understanding the security, privacy and trust challenges," 2010.

[49] R. S. Kumar and A. Saxena, "Data integrity proofs in cloud storage," in Communication Systems and Networks (COMSNETS), 2011 Third International Conference on, 2011, pp. 1–4.

[50] J. B. D. Joshi, E. Bertino, U. Latif, and A. Ghafoor, "A generalized temporal role-based access control model," IEEE Trans. Knowl. Data Eng., vol. 17, no. 1, pp. 4–23, 2005. https://doi.org/10.1109/TKDE.2005.1.

[51] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Infocom, 2010 proceedings ieee, 2010, pp. 1–9.

[52] G.-J. Ahn, M. Ko, and M. Shehab, "Privacy-enhanced user-centric identity management," in Communications, 2009. ICC'09. IEEE International Conference on, 2009, pp. 1–5. https://doi.org/10.1109/ICC.2009.5199363.

[53] X. Zhang, M. Nakae, M. J. Covington, and R. Sandhu, "Toward a usage-based security framework for collaborative computing systems," ACM Trans. Inf. Syst. Secur., vol. 11, no. 1, p. 3, 2008. https://doi.org/10.1145/1330295.1330298.

[54] A. Sedgewick, "Framework for Improving Critical Infrastructure Cyber-security," NIST, 2014.

[55] M. Basso and J. Mann, "MarketScope for Enterprise File Synchronization and Sharing," Gartner, 2013.

[56] N. Grozev and R. Buyya, "Inter-Cloud architectures and application brokering: taxonomy and survey," Softw. Pract. Exp., vol. 44, no. 3, pp. 369–390, 2014. https://doi.org/10.1002/spe.2168.

[57] Z. Xin, L. Song-qing, and L. Nai-wen, "Research on cloud computing data security model based on multi-dimension," in Information Technology in Medicine and Education (ITME), 2012 International Symposium on, 2012, vol. 2, pp. 897–900.

[58] F. Zhao, C. Li, and C. F. Liu, "A cloud computing security solution based on fully homomorphic encryption," in Advanced Communication Technology (ICACT), 2014 16th International Conference on, 2014, pp. 485–488. https://doi.org/10.1109/ICACT.2014.6779008.

[59] H. Suo, Z. Liu, J. Wan, and K. Zhou, "Security and privacy in mobile cloud computing," in Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International, 2013, pp. 655–659. https://doi.org/10.1109/IWCMC.2013.6583635.

[60] M. Alhamad, T. Dillon, and E. Chang, "Sla-based trust model for cloud computing," in Network-Based Information Systems (NBiS), 2010 13th International Conference on, 2010, pp. 321–324. https://doi.org/10.1109/NBiS.2010.67.

[61] V. Mukhin and A. Volokyta, "Notice of violation of IEEE publication principles security risk analysis for cloud computing systems," in Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2011 IEEE 6th International Conference on, 2011, vol. 2, pp. 737–742. https://doi.org/10.1109/IDAACS.2011.6072868.

[62] J. Surbiryala, C. Li, and C. Rong, "A framework for improving security in cloud computing," in 2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), 2017, pp. 260–264. https://doi.org/10.1109/ICCCBDA.2017.7951921.

[63] J. R. Jain and A. Asaduzzaman, "A novel data logging framework to enhance security of Cloud computing," in SoutheastCon 2016, 2016, pp. 1–6.

[64] M. M. Potey, C. A. Dhote, and D. H. Sharma, "Homomorphic Encryption for Security of Cloud Data," Procedia Comput. Sci., vol. 79, pp. 175–181, 2016. https://doi.org/10.1016/j.procs.2016.03.023.

[65] A. Bhardwaj, G. V. B. Subrahmanyam, V. Avasthi, and H. Sastry, "Security Algorithms for Cloud Computing," Procedia Comput. Sci., vol. 85, no. Cms, pp. 535–542, 2016.

[66] G. Brunette, R. Mogull, and others, "Security guidance for critical areas of focus in cloud computing v2. 1," Cloud Secur. Alliance, pp. 1–76, 2009.

[67] Al-hashimi, m. u. h. a. n. e. d., et al. "Address The Challenges Of Implementing Electronic Document System In Iraq E-Government-Tikrit City As A Case Study." Journal of Theoretical & Applied Information Technology 95.15 (2017).

[68] Shakir, M., Abubakar, A. B., Yousoff, Y. B., & Sheker, M. (2016). IMPROVEMENT KEYS OF ADVANCED ENCRYPTION STANDARD (AES) RIJNDAEL_M. Journal of Theoretical & Applied Information Technology, 86(2).