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. 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 economics 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.

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
chose. 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.

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 manipulations 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 the 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-reputation 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 (PCI DSS), and ISO [12][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 present 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 have to 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.

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>
<thead>
<tr>
<th>Inclusion criteria</th>
<th>Exclusion criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Articles related to Security framework in cloud computing implementation written in English.</td>
<td>a) Articles which focus on security issues which are applied in non-cloud computing environments.</td>
</tr>
<tr>
<td>b) Articles which are related to Authentication</td>
<td>b) Articles which focus on authentication model which are</td>
</tr>
</tbody>
</table>

Figure 4: Selection Process of Articles Extraction.

Table 1: Inclusion and Exclusion Criteria
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 development 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%).

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%).

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.

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.

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

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

<table>
<thead>
<tr>
<th>Articles publisher</th>
<th>Objectives</th>
<th>Aspect of authentication model</th>
<th>Articles Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>[24] IEEE</td>
<td>To suggest a cloud security trust model and certain social security</td>
<td>sub-classified into three core groups – multiple stakeholders, open space, and handling of critical information issues</td>
<td>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]. 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.</td>
</tr>
<tr>
<td>[26] IEEE</td>
<td>To determine the best approach to avoid any fraudulent flows</td>
<td>Transport Layer Security (TLS) should be used for the communications between switches and control planes</td>
<td>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.</td>
</tr>
<tr>
<td>[27] Springer</td>
<td>To proposed mechanisms to prevent unauthorized access</td>
<td>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. Supplementary security framework</td>
<td>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). Suggests relevant solutions to already existing issues concerning both cloud providers and users.</td>
</tr>
<tr>
<td>[28] IEEE</td>
<td>To proposed trust model has ability to enhancing</td>
<td>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. Supplementary security framework</td>
<td>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]. 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.</td>
</tr>
</tbody>
</table>

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%).
the standard security.

[29] IEEE
To pinpoint security SaaS concerns
To examine the secure connectivity in cloud computing by reviewing existing network security technologies

[30] IEEE
To proposed authentication model for hybrid cloud computing
Introduce CaaS model (inter- and intra-cloud communication) B2B

[31] ITU
To protect information in the cloud from leaking
That model operates through PKI and a CA system with single data encryption and comprises three main elements

[32] IEEE
To avoid any illegal access to the documents
Secure Authentication Model (SAM)

[33] Scopus
To avoid any illegal access to the documents
Electronic personal synthesis behavior (EPSB)

[34] Scopus
To protect the system from both inside and outside attacks
USBs and Smart Cards

[35] Scopus
To determine when an outside user attempts to login using a proxy gateway and interface
VM interface

[36] IEEE
To protect information in the cloud from leaking
Follow the authentication and confidentiality approach

[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.

[38] IEEE
To propose trust model
Trusted Support Service (TSS)

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

This section presents the main 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

<table>
<thead>
<tr>
<th>Articles and publisher</th>
<th>Objectives</th>
<th>Aspect of authentication model</th>
<th>Articles Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>[39] IEEE</td>
<td>To Prevent Any Fraudulent Operations</td>
<td>1. Authentication. 2. Data Integration. 3. Data Encryption. 4. User protection.</td>
<td>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.</td>
</tr>
<tr>
<td>[40] Indiana Un.</td>
<td>To Ensure the Cloud’s Optimal Security 2. To Diagnose Privacy Risks</td>
<td>1. Effective Privacy Protection Scheme (EPPS) (employs encryption algorithms to diagnose privacy risks)</td>
<td>Increase Cloud Security By 35–50%.</td>
</tr>
<tr>
<td>[22] IEEE</td>
<td>To enhance cloud computing security</td>
<td>To find viable solutions to pending threats and improve the overall safety of the cloud performance</td>
<td>To identify possible security issues in cloud computing and determine the necessary security features and possible solutions</td>
</tr>
<tr>
<td>[41] CNKI</td>
<td>To enhance data security in cloud computing (data privacy)</td>
<td>To find viable solutions to pending threats and improve the overall safety of the cloud performance</td>
<td>To explain data integrity in details and the importance of its maintenance</td>
</tr>
<tr>
<td>[42] SCIELO</td>
<td>To enhance data security in cloud computing (data privacy)</td>
<td>To find viable solutions to pending threats and improve the overall safety of the cloud performance</td>
<td>To explain data integrity in details and the importance of its maintenance</td>
</tr>
<tr>
<td>[43] IEEE</td>
<td>To integrity evaluation technique was discussed. Cloud safety issues were again listed and elaborated on.</td>
<td>To find viable solutions to pending threats and improve the overall safety of the cloud performance</td>
<td>To explain data integrity in details and the importance of its maintenance</td>
</tr>
<tr>
<td>[23], [44], Springer [45]IEEE</td>
<td>To enhance cloud computing security</td>
<td>To find viable solutions to pending threats and improve the overall safety of the cloud performance</td>
<td>To identify possible security issues in cloud computing and determine the necessary security features and possible solutions</td>
</tr>
<tr>
<td>[11] IEEE</td>
<td>The identified problem types are access, cloud infrastructure, data, and compliance</td>
<td>To find viable solutions to pending threats and improve the overall safety of the cloud performance</td>
<td>To identify possible security issues in cloud computing and determine the necessary security features and possible solutions</td>
</tr>
<tr>
<td>[46] IEEE</td>
<td>Proposed security guideline for cloud computing</td>
<td>To find viable solutions to pending threats and improve the overall safety of the cloud performance</td>
<td>To identify possible security issues in cloud computing and determine the necessary security features and possible solutions</td>
</tr>
<tr>
<td>[47] SCOPUS</td>
<td>Prepared preliminary study</td>
<td>To find viable solutions to pending threats and improve the overall safety of the cloud performance</td>
<td>To identify possible security issues in cloud computing and determine the necessary security features and possible solutions</td>
</tr>
<tr>
<td>[48]</td>
<td>To understand risk</td>
<td>Provided a mapping</td>
<td>Risk management in cloud computing can be divided into three levels: level</td>
</tr>
</tbody>
</table>
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,

<table>
<thead>
<tr>
<th>Articles and publisher</th>
<th>Objectives</th>
<th>Security Framework Layers</th>
<th>Papers results</th>
</tr>
</thead>
<tbody>
<tr>
<td>[57] Wiley</td>
<td>1. To achieve better overall Quality of Service (QoS), reliability and cost efficiency by utilizing multiple clouds</td>
<td>Three authentication levels: 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 authorized to use</td>
<td>The authors further proposed a coRBAC cloud authentication model, which supplies the user with three authentication levels upon login</td>
</tr>
<tr>
<td>[58] Accent</td>
<td>1. To improve security framework for cloud computing via web 2. to determine intricate security features in cloud computing</td>
<td>1. Authentication layer; 2. Encryption layer; 3. Privacy Protection 1. Data management</td>
<td>This model allows for better security, as the user has full control when accessing the cloud</td>
</tr>
<tr>
<td>[59] IEEE</td>
<td>1. To improve framework to avoid any attack 2. To pointed out as a possible answer to the cloud computing dependability dilemma</td>
<td>1. Authentication layer; 2. Access control; 3. Encryption layer 1. Authentication layer; 2. Management layer.</td>
<td>Suggest behavioural authentication in contrast to traditional authentication with credentials, certificate or key based authentication</td>
</tr>
<tr>
<td>[60] ACM</td>
<td>To develop security framework for business to protect cloud computing from Viruses and trojan attack</td>
<td>1. Authentication layer; 2. Intrusion detection; 3. Encryption layer</td>
<td>Proposed security framework for business cloud computing based on blending of multilayered security with policy, real services, and business activities have been shown</td>
</tr>
<tr>
<td>[53] ACM</td>
<td>To develop security system for enforcing security in cloud computing</td>
<td>1. Authentication layer</td>
<td>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</td>
</tr>
<tr>
<td>[62] IEEE</td>
<td>To improve accountability in cloud computing</td>
<td>1. System layer; 2. Data layer; 3. Workflow layer.</td>
<td>Proposed a Trust cloud framework. This framework is considered a theoretical framework because it didn’t cover computational demonstrations, case studies, and quantitative analyses.</td>
</tr>
</tbody>
</table>
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%).

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 using cloud services, especially in the case of public clouds.

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-

| [63] IEEE | To avoid failure of any single cloud, encrypt user files. | 1. Authentication layer; 2. 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. The 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. |
| [64] IEEE | To keep track of the genuine usage of end-user’s information in the cloud | Authentication layer | Proposed a homomorphic encryption of data in cloud computing. |
| Elsevier (Science Direct) | To protect storing data in cloud computing | Encryption layer | Presented a brief overview and comparison of Cryptographic algorithms. |
| [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. |
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 unauthorized 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 Yahiya Abdullah, Instructor at Alburaimi University College, as well as Sami Abdullah who helped with the corrections in the English language.

References
