International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/23 Volume 12, Issue 3, May – June (2025)

REVIEW ARTICLE

An Extensive Review of Hosting of Cloud, IoT, and Web-Based Services: Security Issues and Challenges Ahead

Bhupesh Kumar Dewangan
Symbiosis Institute of Technology, Nagpur Campus, Symbiosis International (Deemed University), Pune, Nagpur, Maharashtra, India.
✉ bhupesh.dewangan@gmail.com

Piyush Chauhan
Symbiosis Institute of Technology, Nagpur Campus, Symbiosis International (Deemed University), Pune, Nagpur, Maharashtra, India.
shbichauhan@gmail.com

Received: 08 March 2025 / Revised: 06 June 2025 / Accepted: 16 June 2025 / Published: 30 June 2025

Abstract – In today's era, IoT, and cloud computing are used in all domains for data transition by cost optimization, fast execution, and low maintenance at the user end. In continue to this, all services from different technologies can be opted, if they are secure in terms of reliability, confidentiality, authenticity, and integrity. Security plays a vital role while transmitting data whether it's about IoT-based devices and applications, cloud or self-hosted websites, or any other services. Security of cloud services will be included as a preferable topic for researchers but web service security is also exigent. In this paper, a comparative analysis is presented between IoT, cloud-based, and web-based services based on different research parameters to explore the major issues and challenges while adopting cloud and web services based on various security parameters. For conducting this study, we have considered more than 250 articles from WoS and Scopus databases, out of which more than 100 articles have been included in this study. We have classified the security into 9 parameters and studied each parameter for cloud and self-hosted web services and presented the comparison in tabular form, graphs, and charts. This work aims to observe which of the two services is better. Additionally, open research issues and challenges are discussed in the work.

Index Terms – Cloud-Based Services, Web-Based Services, Security, IoT, Bibliometric Analysis, Firewall.

1. INTRODUCTION

The main components of this review are Cloud, IoT, and Web-services which has been considered to explore various challenges while deploying application in highly secured platform. The integration of the above services is very useful in various applications. The operative procedure of IoT devices are ensure to collect data, and Web services are being transferred those data and trigger the actions between various controlling systems. Data is processed by Cloud computing stores and processes the data, providing scalability and accessibility.

For the past decades, cloud computing is included in emerging technologies due to its characteristics and its services. One can access cloud services with the help of a Cloud Service Provider (CSP) through the internet. Popular CSPs are Amazon, Microsoft Azure, Google, and many more. The appropriate choice of any service provider depends on the need of the user [1]. The growing IT industry requires ample resources, instead of purchasing these resources, cloud computing provides these resources as streamlined and at a cheaper cost to the client efficiently [2] [3]. If a person is interested in using cloud services, then he just needs a machine with no special configuration and a good internet connection. As the data is stored and communicated through the internet, then it becomes necessary to make the transmission secure.

Security in the cloud is the main concern either in terms of data storage or efficient data access [4] or something else. The design and architecture of cloud computing exposed numerous organizations to several attacks. The approach of different cloud deployment and service models are used to provide data access to the users from cloud storage [5] [6]. One of the main challenging tasks is to involve third-party for data handling [7]. To ensure the security a trusted third party is introduced which ensures confidentiality, authentication, and integrity. Secure transmission of data over the network is a complex issue [8]. Moreover, various layers of the cloud are vulnerable to typical attacks and threats [9], like the two core layers that are the application layer and the platform layer are prone to attack [10]. Besides the different layers, the services

REVIEW ARTICLE

of the cloud are also vulnerable to attacks like Software as a service (Saas) [11]. One example of an attack is the DOS attack, it causes websites in a nonworking state for a long period, it can cause much damage to the cloud computing environment. This can cause high damage to the cloud as the cloud resource become unavailable [12]. Another example of an attack is the authentication attack. It occurs between the cloud platform and end-users. To avoid unauthorized access from the servers, cryptography keys are used [13] [14]. Using identical tokens, malfunctioning of the servers can be identified in cloud data security and because of this block-level security design is introduced [15]. In comparison with private clouds, public clouds are more prone to external threats [16]. Mitigation measures and restrictions are poor or do not exist, which results in internal threats to public clouds [17] [18] [19] [20].

1.1. Motivation

Trust is the main key to opt any web services from service providers. Due to different security challenges and issues most of the users are distracted from online services [21]. To investigate this, Authors Alloghani et al., conducted the study on security challenges in cloud, including investigation studies, reports, features, and generic information. In his work, he discussed the relative research from 2014 to 2020 and classified all of them based on various parameters such as type of document, year-wise article distribution, journal-wise, and so on [22]. Author Kim J. et al., proposed the solution to such challenges one of the authors providing efficient and flexible security to consumers without installing security equipment [23]. In continuation, Yassin W. et al., proposes a new service of cloud which is based on Intrusion Detection. This system detects malicious activities over the network and can also be implemented for public and private cloud [24].

It can be concluded that security in the cloud is one of major area that need to be address. In this paper, an investigation has been conducted on cloud-hosted services based on the most useful parameters like authentication, password security, CAPTCHA generation, and others. To be more focused, not only cloud web services, the self-hosted web services also has been considered for different security issues, and compared with the cloud web services, to understand the best choice based on the consumer's need. In this investigation, more than 100 research works have been considered to conduct the comparative analysis between both the services and the outcomes are presented in graphical form by the countries of the research, year of publication, publishers, and others with different challenges with possible solutions. In table 1, the basic difference between Cloud, IoT, and web services are presented.

Table 1 Comparative Analysis Between Cloud vs IoT vs Web Services

Feature / Parameter	Cloud Computing	IoT	Web Services
Definition	Delivery of computing services via internet	Network of physical devices connected online	Standard protocols to enable software apps to interact
Usage	Storage, computing, software as a service	Automation, real-time monitoring, data collection	Data exchange and application communication
Technologies	Virtualization, APIs, containers, orchestration	Sensors, microcontrollers, connectivity (Wi-Fi, Zigbee, etc.)	SOAP, REST, HTTP, XML, JSON
Communication	Server-to-server / Client-server	Device-to-device / Device-to-cloud	Application-to-application
Data Handling	Scalable storage and processing	Real-time data capture and transmission	Structured communication using protocols
Examples	Google Drive, AWS EC2, Azure SQL	Smart thermostat, fitness tracker	Google Maps API, Amazon Product Advertising API
Interdependence	Supports IoT by providing infrastructure	Uses cloud for storage and processing	Used in both IoT and cloud for integration
Security	Data breaches, misconfigured cloud settings	Device security, privacy, data integrity	Authentication, encryption, data validation

The integration of Cloud, IoT, and Web Services are as follows:

These three technologies often work together in modern IT ecosystems:

- IoT devices collect data.

REVIEW ARTICLE

- Web services transfer data and trigger actions between systems.
- Cloud computing stores and processes the data, providing scalability and accessibility.

The Workflow of these technologies can be understood through Figure 1.

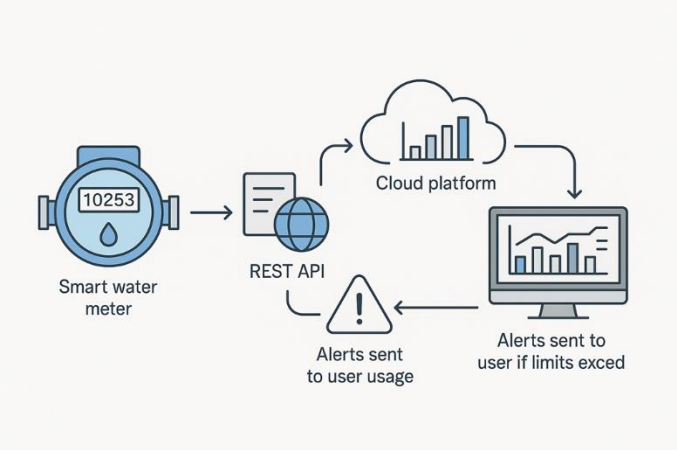

Figure 1 Integration of Cloud, IoT, and Web Services

The section 2 is deal with the related work and it is categorized into twelve sub section, in continue with this section 3 deals with comparative analysis of cloud, IoT, and Web Services based on various parameters. Section 4 explains the various issues and challenges while deploying these technologies with some open research problems, and section 5 conclude the overall discussion.

2. RELATED WORK

In this paper, more than 250 related research articles have been studied, out of which more than 100 research have been included. This section includes the literature review based on research parameters. These parameters are being researched for the cloud and as well as for web services too. Further, Section 3 consists of detailed comparative analysis in the form of tables, graphs, and charts. After an in-depth analysis of Section 3, Section 4 presents the open research issues and challenges. At last, section 5 concludes the work. The review approach has been shown in Figure 2. The following area has been classified while conducting the investigation, and analyzed the different aspects between cloud and web-services.

Before discussing the literature review, the research parameters are mentioned below:

- IoT Cloud-based model
- Generation of Public or Private key or Cryptography
- Generation of Certificate and validation
- Self-protection
- Secure logging
- Spam filtering
- Data storage and protection
- Password hashing and storage
- CAPTCHA generation with its verification
- Software widgets like password strength meter
- Security Scanner
- Firewall

Now, the literature review is based on these parameters discussed below:

2.1. IoT-Cloud Based Models

This section includes the study on the current issues of IoT Cloud-based models and their applications. Based on the current study conducted by Chen, F. et al., IoT Cloud models [25] are categorized into 10 categories as follows:

Web camera: The flash memories and their interfaces are unprotected; however, the password is hardcoded, but still at the time of communication it uses plain text API's which can be the reason of data leakage which unveiled the user privacy.

Healthcare facilities: In such applications, password strength is generally not good, also the memory card is unprotected, in some extent, this can be the cause of unveiled the privacy of the users.

Smart Plugs: Plain text APIs in common LAN; insecure protocol; Weak authentication; firmware is unprotected.

Baby monitor: Plain text APIs used; data stored in clear text; weak authentication; hardware's are not protected; weak authentication in IoT Cloud devices.

Industrial Equipment: Hardware are unprotected; weak interfaces; weak data privacy and protection.

Smart Home: Large encrypted files, unnecessary data monitoring, and collection; weak privacy handling.

Human factors: Privacy concerns; data transmissions are not secured; poor authorization; data removal issues.

Children's Toy: multiple uses of POST token; authentication is poorly defined; privacy leakage while HTTP response.

Smart-Things: Control over interoperability is insufficient; control over access issues; one-to-one authentication technique; cloud and its user SMS handling issues.

Smart-Voice Assistant: Third-party handling issues; recognition of voice; user identification is tough; similar private key over the cloud.

REVIEW ARTICLE

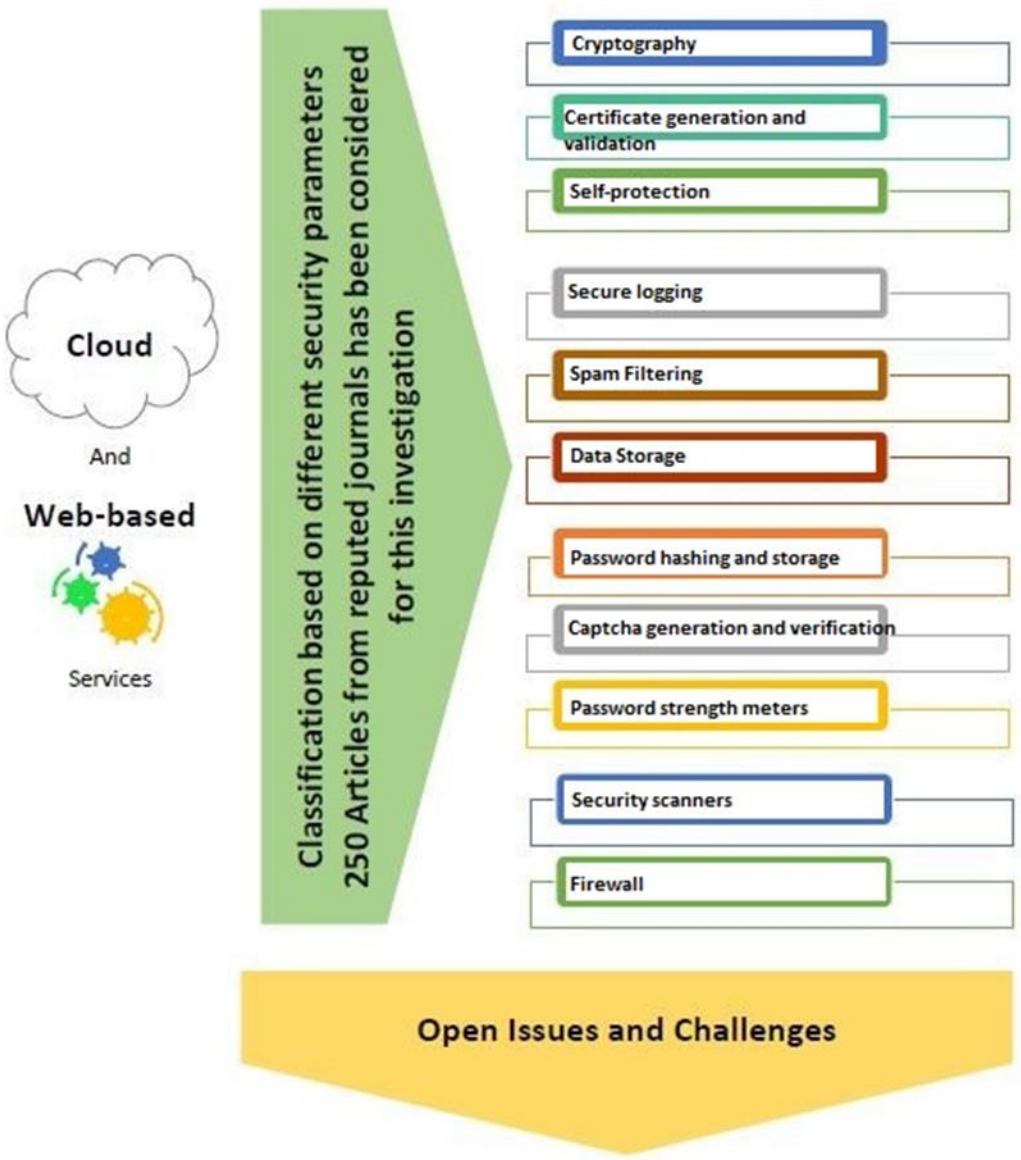

Figure 2 Review Approach

2.2. Generation of Public or Private key or Cryptography

Figure 3 presents an overview of the above work, i.e., a comparison between services based on cloud and web by cryptography.

Many authors described a few standard cryptography techniques along with hybrid techniques of cryptography. Author Chaudhary, compares the efficiency of both and concluded that hybrid algorithms are more efficient for any procedure [26]. In continue to this, another author Kumar, introduces a combination of RSA and DES algorithms to improve the system's security for IoT applications and data storage in the cloud [27], where, author Mahalle, combines RSA and AES and uses three different keys in cryptography and a unique key generation method [28]. Sengupta proposes a hybrid encryption method that provides security to the cloud over the server, at the client's location, and over the network. This system is designed so that the hacker will take more time for decryption compared to others [29]. An efficient method based on the RSA algorithm is used by the author to increase the security of stored data in the cloud [30]. For increasing the data security, the author presents an asymmetric and symmetric algorithm, i.e., RSA and AES, and then after the encrypted data is hidden in an image using the LSB algorithm. Moreover, test images are tested which results in improve data compression, next, in the phase of data validation SHA algorithm is used

REVIEW ARTICLE

which overall results due in high data security [31]. Gugnani explained that while using cloud-based services, confidentiality is enhanced for the end-users by implementing DNA encryption in it. The main focus is to protect the XML document from inappropriate information disclosure [32].

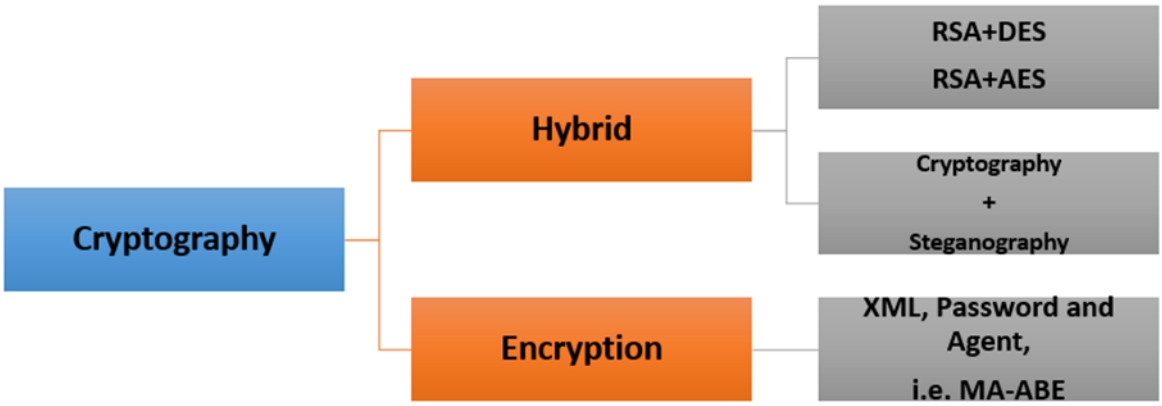

Figure 3 Comparison Between Services, Based on Cloud and Web by Cryptography

Other than hybrid algorithms, the authors propose variant methods for cryptography one author introduced encryption based on a password to protect sensitive data. Without storing a user's password, the user is authenticated with the help of encryption or decryption keys. Moreover, the performance matrices are investigated in the study. The experimental results for the same are shared [33]. For the access control mechanism in the mobile cloud computing environment, the author proposes MA-ABE which is agent-based. Both dynamic and static attributes are used for the encryption of data. Moreover, in the presented work, the secret key is used and the proposed work is compared with the previous under certain parameters [34]. For hybrid cloud services, the authors should discuss the various means of password encryption [35]. For protecting users' data, authenticating the user before data access, establishing secure channels, and data encryption are suitable [36]. Another author analyzed the risk of data security over the cloud and thus proposes encryption as a service using a private cloud, which eliminates the security risk and reduces the encryption inefficiency on the client side [37].

Besides, cloud key generation for websites is also discussed by the authors. Gondaliya proposes a hybrid RSA which combines two different keys, that is, the combination of the private with the public key for both encryptions as well as for decryption. This is then compared with RSA and ERSA [38]. The author presented the communication between the client and server using a targeted symmetric key using the first, second, and third data structure [39]. Other authors propose an advanced algorithm that combines cryptography and stenography for enhancing the security of private information. It also uses Unicode for the same. Arabic text is used for stenography and the result shows that the scope of Arabic carriers is increased [40]. Hao focuses on the security of data communication which is based on XML. This model is for sender-side encryption which can encrypt the signature [41].

2.3. Generation of Certificate and Validation

Figure 4 presents an overview of the above work, i.e., a comparison between services based on cloud and web by certificate generation and validation.

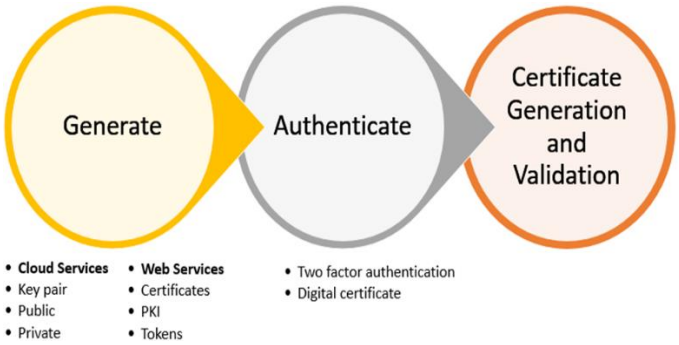

Figure 4 Comparison Between Services Based on Cloud and Web by Certificate Generation and Validation

For certificate generation, the author implemented Trusted Computing Technology for the certification of cloud services [42]. The author provides a certificate generation method that uses key pairs. This pair is the combination of a public key with a private key. This pair of keys is used for signing the certificate, the end-user is validated during the signing window. If the window is expired, then the key pair is discarded for that particular end-user [43]. Another author introduces an advanced framework that increases data storage security and protects it from unauthentic access with the help of ADC (Associated Digital Certificate) for accessing cloud services the user must have encrypted, decrepit, and other certificate options. Authentication of the user is initiated by the checking of the public key, followed by verification of the role in ADC then after the digital signature is provided. After validation of the secret key, the user is permitted to access the secured files

REVIEW ARTICLE

[44]. Seo worked on the problem of encryption based on identity and certificate revocation. For this, they proposed a certificate-less encryption method without pairing. Presented experimental results show that the proposed approach is more efficient [45]. Chakraborty introduces biometric authentication with two parameters to enhance security. In this system, a digital signature is generated and verified on the cloud. The two factors used for authentication are biometric authentication and a one-time key. Without verification of these two, a user will not be authenticated [46].

Besides, cloud certificate generation for websites is discussed by the authors like, as described how they built let's encrypt and the automated system for interaction and certificate generation. Let's Encrypt be included in the world's largest CA for HTTPS, which issues millions of certificates at low cost or no cost. They also described the popularity of the CA all over the globe [47] i.e introducing a security token mechanism to generate a digital certificate. PKI key pair is installed with the digital certificate for verification. If this gets validated, then only the certificate is generated [48]. Harn introduces a digital certificate for authentication of the user which is generalized. This certificate does not consist of any public key of the user, rather than this it entails birth certificate information, driving license information, etc. It is used as a secret token. Protocols based on discrete logarithm and integer factoring are used to achieve authentication [49].

2.4. Self-Protection

Figure 5 presents an overview of the above work, i.e., a comparison between services based on cloud and web by self-protection.

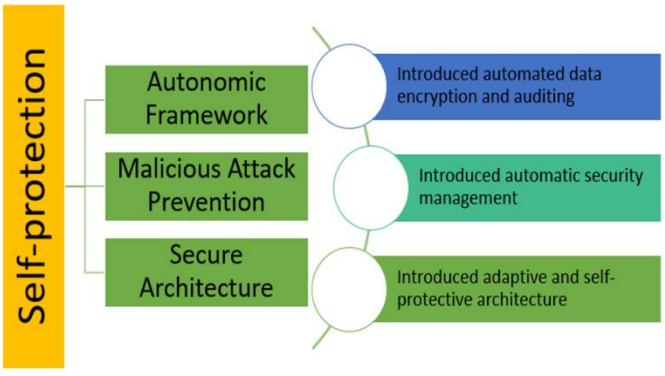

Figure 5 Comparison Between Services Based on Cloud and Web by Self-Protection

For self-protection, an automated framework is presented by the authors for increasing security in the cloud. The user's data is encrypted automatically to preserve its confidentiality. To maintain data integrity, automatic data auditing is presented. After this, automated decryption of data is used [50]. The proposed method provides self-protecting security from malicious attacks to provide continued services to authenticated users and is named this approach as SECURE. Experimental results showed that the approach works efficiently for false rate and intrusion detection [51]. Another author analyzed the new mechanism and implements the same, also the results of experiments show that the introduced system is efficient and improves access control [52]. Another author proposes a method where data protection is ensured in two ways while the transmission of data. To achieve self-protection, the author uses active data bundles for access control, that is fine-grained encryption by the attribute is used and for the management of secure key RSA threshold is used [53]. Another author proposed the idea of adaptive network architecture which is self-propagating for multi-agent [54]. An architecture based on self-protection is proposed, which overcomes the limitations of the previous work. The proposed architecture provides security at two levels, i.e., both across and within the infrastructure layers. In addition, the introduced security policy is flexible [55].

Along with the cloud, self-protection is also introduced for websites. Yin analyzed script injection vulnerabilities and implemented an algorithm to enhance the security of web pages. Injection filtering is automatically inserted into the web program by it. By analyzing the flow of data, filters are automatically inserted, which results in the self-protection of the web page [56]. The author proposes an adaptive and secure self-protecting architecture for Denial-of-Service attacks. For business quality and context, reasoning based on utility is used. Rainbow's self-adaptive framework is used in the work [57]. For protecting the computing system in a network, the authors introduced automatic security management which detects, identifies, and estimates the attacks and takes a sequence of effective actions for protecting the computing system. Experimental results showed that the automated security system can defend against various types of attacks efficiently [58].

2.5. Secure Logging

Figure 6 presents an overview of the above work, i.e., a comparison between services based on cloud and web by secure logging.

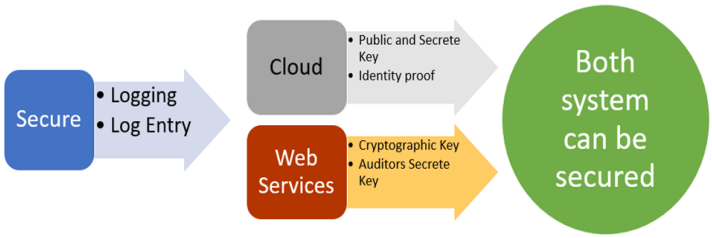

Figure 6 Comparison Between Services Based on Cloud and Web by Secure Logging

For upgrading secure logging as a service, an author can assist it through blockchain which is capable of handling multi-stack

REVIEW ARTICLE

holder collision problems. It ensures integrity by the property of blockchain i.e., immutability along with confidentiality [59]. A secure logging framework is introduced in the work of another author. Signing and verifying of log data were implemented and evaluated on it. For the logged user, the public key is utilized to validate the integrity, the secret key is used for the generation of signatures of the log [60]. We proposed a secure logging service where identity proofs are generated in real-time. If the identity proof is generated by a dishonest CSP, then it can't manipulate or remove the logging data [61]. Kunz introduces the secure logging method with a secure database of log files. This method could resist internal manipulations, thus creating confidentiality [62]. This method gives a solution for certificates of data processing that are alleged to secure log management that is based on the cloud and introduces a framework for it using anonymous protocols. The security issues are discussed in the work during all phases of the log. One of the distinctive challenges is outsourcing log management [63]. Zawood introduced and implemented secure logging as a service for network logs, which ensures the confidentiality of the cloud users. Furthermore, to preserve the cloud's integrity, proofs of previous logs are recorded [64]. Rajalakshmi analyzed the problem and challenges of secure logging and introduced homomorphic algorithms as a solution. The proposed framework fulfills confidentiality, integrity, privacy, and correctness [65]. The website also implements secure logging; the author worked on the detection of fraud certificates and introduced certificate transparency for logging through cryptography. It is based on Merkle tree hashing along with authentication. Two security goals are achieved in the work, which is secured against malicious loggers and malicious monitors [66]. Another author proposes a method to protect sensitive data. It secures the log entry by encrypting the random cryptography key and the auditor's secret key. Moreover, the fake key is encrypted by using the secret key of the auditor [67].

2.6. Spam Filtering

Figure 7 presents an overview of the above work, i.e., a comparison between services based on cloud and web by spam filtering.

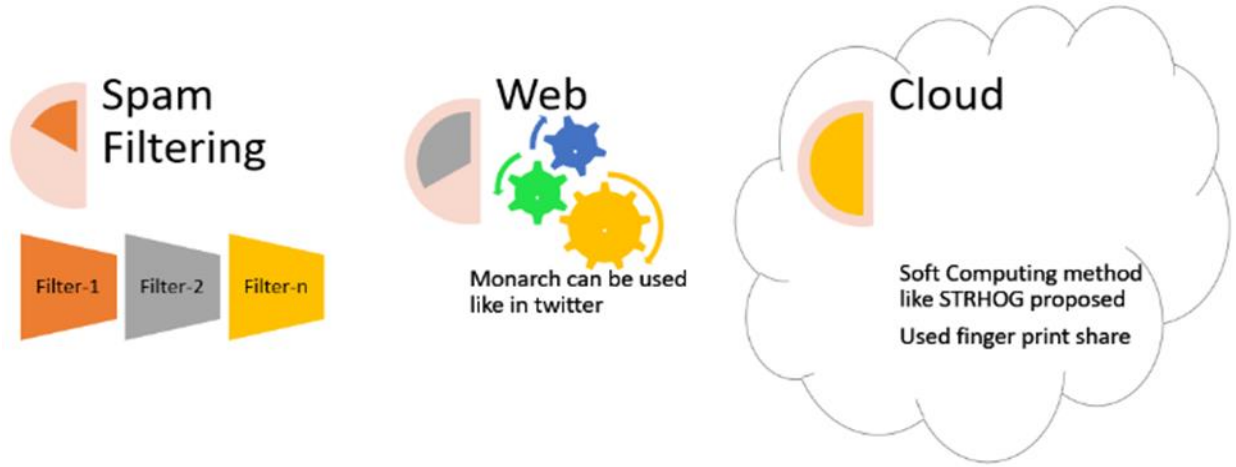

Figure 7 Comparison Between Services Based on Cloud and Web by Spam Filtering

Spam filtering is an important security measure. For this, an author analyzed the two main problems, that is, data protection and data filtering for data owner and data recipient, respectively. Spam image is detected with the help of soft computing methods for intelligent character recognition. The authors analyzed the problem of HOG and overcame it by proposing STRHOG. This improved method helps in beneficial in intelligent character recognition and the nearest neighbor classifier is used by the authors to present a fair comparison between the proposed and the existing one [68]. Aun studied different techniques and challenges of spam filtering. Additionally, spam filtering based on the server is deployed on a cloud environment for the test which results in a bad impact on scalability. To address this issue, a framework is proposed for cloud spam filtering which is scalable [69]. She studied the problem of bulk spam. They proposed a method in which spam is filtered on clouds with the help of fingerprint sharing [70]. Spam filtering for web services like social media is also important. For this, an author discussed the challenges caused by diversity in web service spam. He presented that Monarchies can come up with accuracy and protection but this cannot be generalized. Moreover, they found that spam purposing emails are different from spam campaigns purposing Twitter. The result shows Monarch's scalability and this can protect Twitter-like service [71]. Additionally, another author proposes a method for spam message filtering for Twitter [72].

2.7. Data Storage and Protection

Figure 8 presents an overview of the above work, i.e., a comparison between services based on cloud and web by data storage.

REVIEW ARTICLE

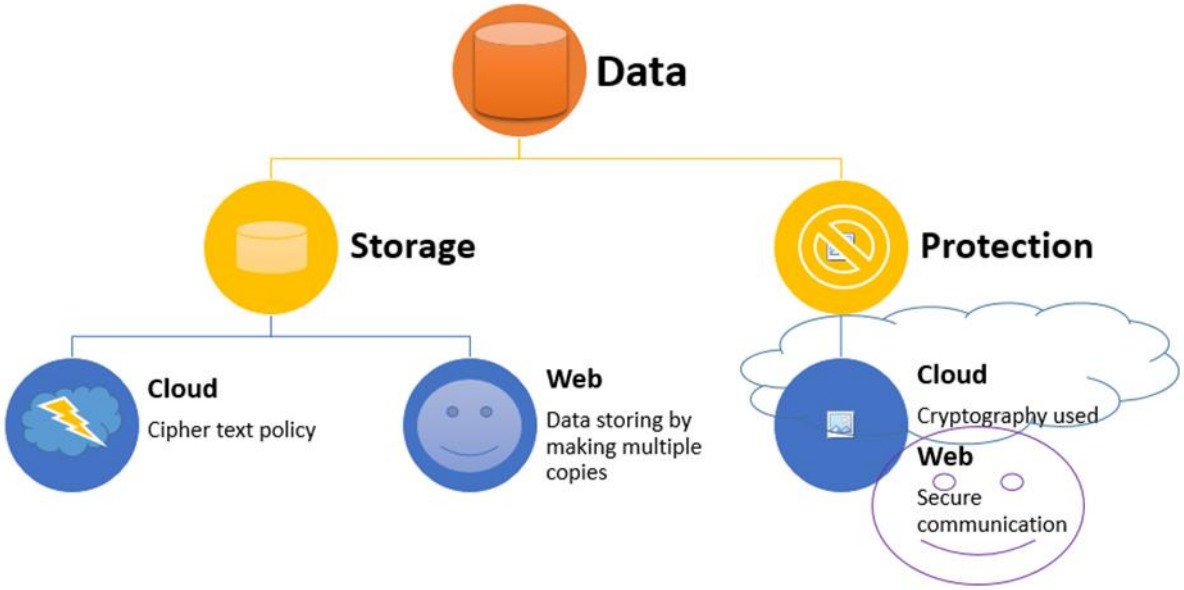

Figure 8 Comparison Between Services Based on Cloud and Web by Data Storage and Protection

Author Odun studied data storage in the cloud. Issues on the services of cloud storage were discussed in the work along with the trends of cloud storage. At last, the author provides a comparative analysis between IBM cloud object and Amazon S3 [73]. The author proposes a flexible method for data storage in the cloud which is encryption based on the cipher-text policy which makes user revocation efficient. This is implemented by using the policy of the user group. Moreover, to avoid a collision attack, a certificate is attached to the private key of the user. The result shows that the computation cost is comparatively low for limited resource devices [74]. Another author studied storage as a service for enterprise solutions and explained its pros and cons. From this paper, it can be concluded that storing data on the cloud is more beneficial than local server storage [75]. An intelligent cryptography method is proposed by Li, through which partial data cannot be reached by cloud providers. It divides the files and stores them on distributed servers. AD2, SED2, and EDCon algorithms are included in the work [76]. Hu proposed a secure scheme of access control for the storage of big data in the cloud. This scheme is based on the NRTU cryptosystem. It overcomes the failures of the original NRTU. The cipher-text is updated with the updated access policy précised by the data owner, this also helps in the validation and recovery of plain text [77].

Secure data storage on websites is as important as securing data on the cloud. For the same, the author presents a communication system where the user needs not to communicate with each server individually. Besides, the information is communicated between the first and second servers. The first request is received by the first web server and then after any one of the second web servers receives the request from the first web server [78]. Fanli introduced a method of storing data by making copies of it and storing them in different blocks. These copies are periodically checked as per the recent importance level [79].

2.8. Password Hashing and Storage

Figure 9 presents an overview of the above work, i.e., a comparison between services based on cloud and web by password hashing and storage.

For achieving confidentiality, the password needs to be secure. Madabatulla enhances the security of OTP by implementing one more layer which comprises special information of the user. This system consists of four-layer protection that is secure, traditional, highly sensitive, and responsive [80]. A method is proposed which can detect frequent and infrequent patterns of passwords, which results in a validation system and uncommon password creation. Its overall results in improved password strength [81]. The author studied different password hashing techniques with practical proofs that are GPU based. With the help of cloud computing, password hash dumping is also investigated. A comparison between the cracking time of distinct password hashing is provided in the paper [82]. For hybrid cloud services, the author discusses various means of password encryption. Data owner and data receiver encryption are also discussed using hash functions and diagrams for the same are provided. In the work, a prevention system is presented against the Brute-Force attack. Using the hash function, a new cryptographic key is generated which makes the system secure, and to enhance it one time a password is also used. The result showed that not a single time the proposed system is unsuccessful in protecting against Brute-Force attack [83]. Proposed password management approach which does not

REVIEW ARTICLE

store passwords like others, three parameters are used in it to identify the user who is stored on a local device [84].

End users are interacting with websites too, so password security on web servers is also required. In the work, Machine learning is used. Existing passwords are used to train the machine and then the passwords are categorized and created after which the strengths of the passwords are calculated [85]. The default framework of web applications and CMS settings are essential for password protection. Password guessing types of attacks are formulated with hashing schemes for famous CMS along with web applications discussed. The study concludes that the majority of CMS and web application frameworks use antiquated hash functions [86]. The author enhances the security of the website by providing a random hash function to the user. They address the problem that if in case a database is hacked then the salt can be cracked after being easily identified. That's why salt is variable or continuously changing and hidden [87]. For the data protection of the information system, two-component authentication is used. The first is a one-time password that is time-based and another is SHA1. The result shows that the proposed system is secured against attacks. Test results show that 30 seconds are sufficient to prevent a hacker's logging in [88].

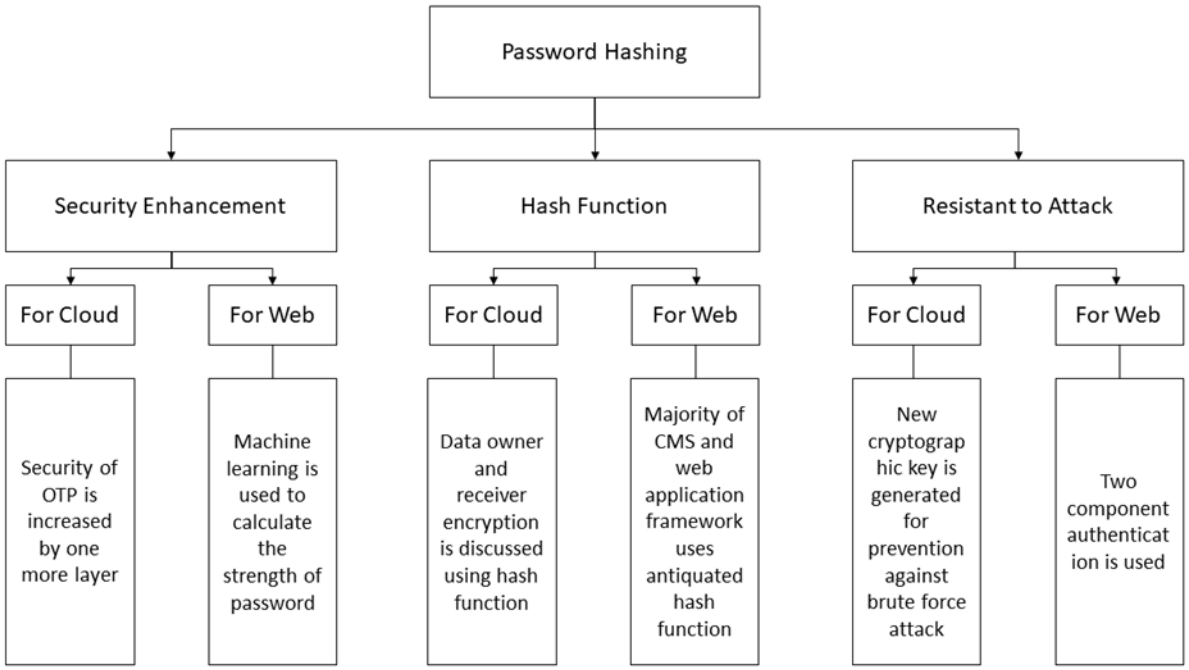

Figure 9 Comparison Between Services Based on Cloud and Web by Password Hashing Storage

2.9. CAPTCHA Generation with its Verification

Figure 10 presents an overview of the above work, i.e., a comparison between services based on cloud and web by CAPTCHA generation for its verification.

Besides, passwords, CAPTCHA generation, and verification need to be secure. The author proposes a hybrid captcha method for implementing multilevel authentication of users. It defines an advanced category of cognitive captcha [89]. Another author focuses on the copy puzzle CAPTCHA and used supervised learning for the detection of bots. Access logs and previous attacks, by adding flags to them, are used as the training dataset. The result shows high accuracy and better performance of the proposed system [90]. Althamary introduced a new method for authentication where a user's password is combined with a CAPTCHA to generate a new passkey. It results in being resistant to various types of attacks and the problem of password guessing [91]. A configurable and robust CAPTCHA service based on the cloud is proposed in the work. It uses hand gestures that are animated to present the sequences of characters [92]. Improved CAPTCHA generation for mobile devices is introduced by the author, which uses distributed verification. It also leads to less response time for a user [93]. For a long course of time, CAPTCHA is used for securing web servers. The author proposes a method that uses linguistic CAPTCHA, it is generated using the language of a particular region that will be difficult for an automated bot to crack [94]. CAPTCHA based on an image is introduced by das along with multiple choice questions on the given set of images which results in a higher level of difficulty for bots to crack.

REVIEW ARTICLE

This CAPTCHA is generated by implementing deep learning [95]. Another author proposed a robust CAPTCHA generation method that uses a modal completion to enhance the security of CAPTCHA. Aftereffects and colors are added to enhance its visibility [96]. For protection against smart bots, Torky proposes Necklace CAPTCHA which is based on an image and generates its test result on a necklace graph. The result proved that the introduced system is more efficient and more secure than the compared ones [97].

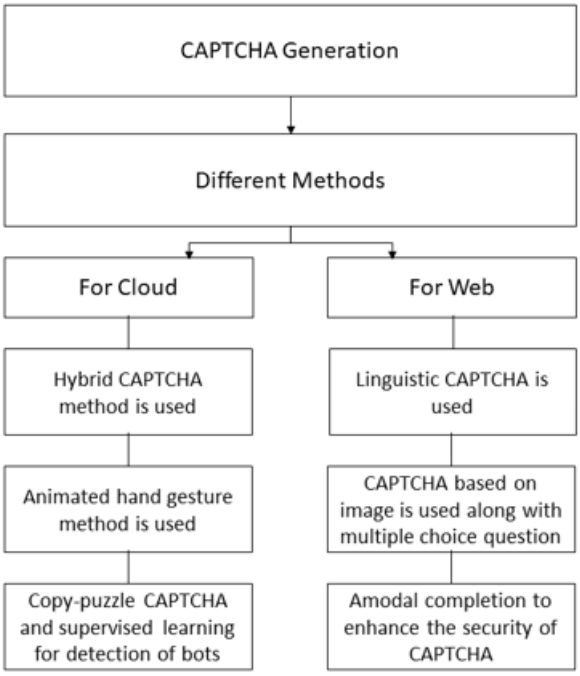

Figure 10 Comparison Between Services Based on Cloud and Web by CAPTCHA Generation with its Verification

2.10. Software Widgets Like Password Strength Meter

Figure 11 presents an overview of the above work, i.e., a comparison between services based on cloud and web by password strength meters.

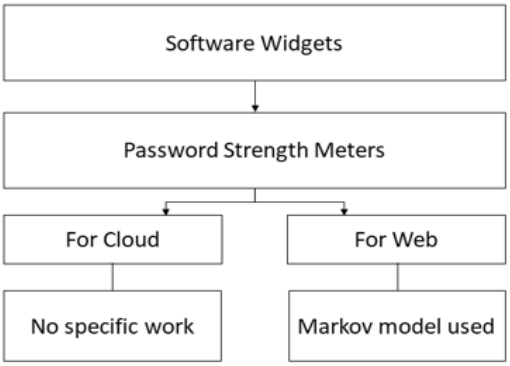

Figure 11 Comparison Between Services Based on Cloud and Web by Password Strength Meters

After studying the existing problem of password security for websites, researchers have made a password strength meter that tells whether the chosen password is either durable or not or the time taken to crack it. Tabular analysis of Password meter websites is also presented in the work [98]. The author proposed a password strength meter which is based on the Markov model. Mathematically, it shows that this model prevents the attack of password guessing and shows improved results in terms of accuracy and security [99]. Sachin introduced a password strength engine which is used to calculate the strength of the password. The complexity of the password is calculated and with the help of the protection function, the estimated cracking time is also calculated [100]. Evernote note-taking application is discussed in the work in which the password strength meter is used to create secure passwords for the user [101].

2.11. Security Scanner

Figure 12 presents an overview of the above work, i.e., a comparison between services based on cloud and web by security scanning.

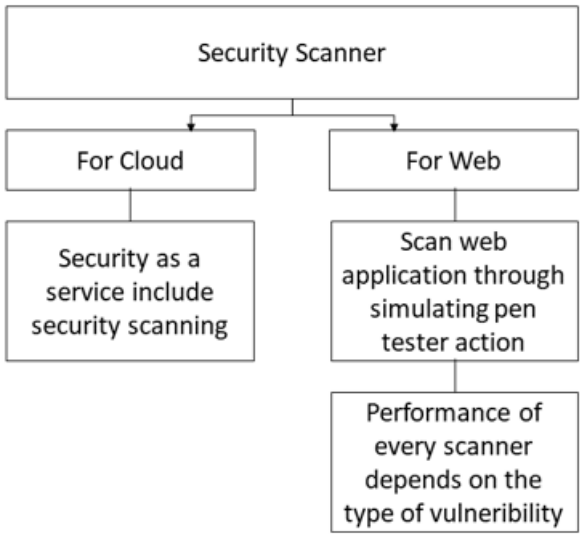

Figure 12 Comparison Between Services Based on Cloud and Web by Security Scanning

For a cloud computing environment, security scanning is achieved by using security as a service and for web applications, effective security scanners are proposed like Andrain developed security scanner to incorporate security problems [102].

Another author Seng scan the web application by simulating pen tester action. It penetrates web application attack strings [103]. Also, Idrissi evaluated different WAVSS based on their effectiveness and it was concluded that the performance of every scanner depends on the type of vulnerability [104].

REVIEW ARTICLE

2.12. Firewall

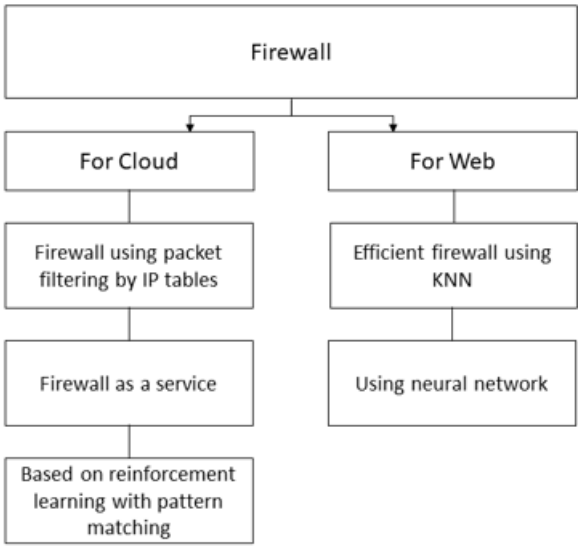

Figure 13 Comparison Between Services Based on Cloud and Web by Firewall

Figure 13 presents an overview of the above work, i.e., a comparison between services based on cloud and web by Firewall.

Authors proposed different types of firewalls for cloud computing environments like Hempfling and did a detailed study and implementation of firewalls using packet filtering by IP tables for cloud computing [105].

Dezhabad introduced a firewall as a service that is implemented in the environment of cloud computing virtualized network functioning. Auto scalability of a firewall that is dynamic is proposed in it [106]. Additionally, praise the proposed firewall that is based on reinforcement learning with pattern matching [107]. Another author introduced for smart grid networks DDOS attack is prevented by the proposed open flow firewall [108].

For web applications, the author thoroughly discussed the benefit of a web application firewall with an overview of models of traffic filtering [109]. Sahin worked on an efficient firewall, a system is proposed by implementing KNN, and efficient results have been achieved [110]. Ito proposed a system that overcomes the problem of different malicious attacks by using the approach of character level convolution neural network which gives accuracy up to 98 percent [111].

In this section, most relative worked done by the researchers has been addressed. Over 100 research has been considered and discussed in various categories in this review. The novelty of this reviews is to identify and categorized the comparative parameters into twelve different categories as discussed above. The comparative analysis and bibliometric analysis of recent work in the research filed has been discussed in the next section.

3. COMPARATIVE ANALYSIS

A thorough study of several papers is being conducted in this paper. These papers are studied with different research parameters. Furthermore, both cloud-hosted and web-hosted services are discussed. A comparative analysis of both hosted services was also discussed by a few authors in 2010 Molnar compared and analyzed the cost and benefits of both cloud-hosted services and self-hosted services. Furthermore, the threats, countermeasures, and shared infrastructure of cloud hosting were described. This study concluded that the cloud is economic in terms of cost and elasticity compared to self-hosting infrastructure presented by these research parameters [112].

In 2015, Ravichandran proposed an automated tool that migrates a website from one hosting architecture to another. The first server architecture consists of services that are specific for one website and the second one consists of plural services to multiple machines and unaffiliated websites [113] and in 2017, Lorenc compares IAAS with traditional web hosting in terms of its cost. Three distinct types of sites are analyzed during the work. It was concluded that in terms of availability and Resilience both are same. For the selected sites, traditional hosting comes out to be better than cloud in terms of cost [114].

Only during these years, the above authors compared cloud-hosted services with web-hosted services. After that, no specific work is found in this area. So, this work aims to focus on a detailed comparison between these two.

3.1. Review Outcomes

In this review, a detailed comparative analysis between cloud-hosted and web-hosted services is presented by the research parameters. Table 2 and Table 3 present the comparative analysis of cloud and web hosting services based on different security parameters as classified by SLR.

Most of the research papers consist of comparative analysis in the form of tables. In this work, the comparative analysis is presented in the form of graphs and charts. This analysis is done on several bases like the related work done in different countries, related work done from the year 2010 to 2020, and more. From this type of analysis, a few conclusions have been made which are discussed in the next section. These graphs are presented in Figures 14 to 16.

Figure 14 presents three field plot captures of the authors who worked on the mentioned research parameters or the related research keywords that are included in the work from 2010 to 2020. Most cited journals are included in this graph. The included authors belong to different countries and published their work in different journals. It can be concluded that:

REVIEW ARTICLE

Most of the authors are interested in cloud-hosted services. Another prominent topic among the authors is the Internet of things and web-hosted applications. The least prominent topics are the rest of the research parameters.

Table 2 Comparison Between Cloud-Based and Web-Based Services Based on Cryptography, Certificate Generation, Self-Protection, Secure Logging, Spam Filtering, and Data Storage

Parameters	Criteria	Pros and Cons	Cloud-Based Services	Web-Based Services
Cryptography	Hybrid method	Pros	Combination of RSA and DES [27] or a combination of RSA and AES [28][31]	Combination of cryptography and steganography [40]
		Cons	Only a combination of RSA with others is found	Combination of RSA with others not found
	Encryption based	Pros	Password [33] and Agent i.e., MA-ABE.[34]	XML based encryption [41]
		Cons	-	Passwords are not used
Certificate Generation	Generation	Pros	Key pair, the combination of the public and private key, is used for it [43]	Automated certificate generation [47]
				Security token mechanism using PKI pair is used [48]
		Cons	No automated framework for certificate generation	Key Pairs are not used
	Authentication	Pros	Two-factor authentication details biometric authentication with one time key [46]	A generalized digital certificate is used for user authentication [49]
			Associated Digital certificate is used to prevent unauthorized access [44]	
		Cons	Generalized and multi-factor authentication not found	Multi-way authentication not found

REVIEW ARTICLE

Self-protection	Automated framework	Pros	Automated `data encryption and data auditing [50]	Automatic security management detects, identifies, and estimates the attacks and takes a sequence of effective actions for protecting the computing system [58]
	Malicious attack	Pros	For intrusion detection, an approach namely SECURE is used [51]	An adaptive and secure self-protecting architecture for Denial-of-Service attacks is introduced [57]
		Cons	Worked only on a few types of Attacks	Worked only on a few types of attacks
Secure-logging	Secure log entry	Pros	Public and secret key is used for signing and verification of log data [60]	Secures the log entry by encrypting random cryptographic key and auditors secret key [67]
			Identity proofs are used for secure logging [61]	
		Cons	Most researchers worked on encryption only	Most researchers worked on encryption only
Spam- filtering		Pros	Soft computing methods like STRHOG are proposed [68]	Monarch can be used to protect Twitter-like services [71]
			Fingerprint sharing is used for spam filtering [70]	
		Cons	-	No robust system
Data storage	Data storage	Pros	Encryption based on cipher-text policy [74]	Storing data by making copies of it and storing them in different blocks [79]
		Cons	Copies are not maintained	Encryption is not used

REVIEW ARTICLE

	Data protection	Pros	An intelligent cryptography method is proposed through which partial data cannot be reached by cloud providers [76]	Communication system where the user needs not to communicate with each server individually. Besides the information is communicated between the first and second server [78]

Table 3 Comparison Between Cloud-Based and Web-Based Services Based on Password Hashing, CAPTCHA Generation, Software, Widgets, Security Scanner, and Firewall

Parameter	Criteria	Pros and Cons	Cloud-Based Services	Web-Based Services
Password hashing	Security enhancement	Pros	Security of OTP is increased by implementing one more layer [80]	Machine learning is used to calculate the strength of the passwords [85]
		Cons	Machine Learning not implemented	Worked only on password strengths
	Hash function	Pros	Data owner and data receiver encryption is discussed using hash functions [35]	Many of the CMS along with web application frameworks implement antiquated hash functions [86]
CAPTCHA Generation	Different methods	Pros	Hybrid captcha method for implementing multilevel authentication of user [89]	Linguistic CAPTCHA is used [94]
			Animated hand gestures are used for CAPTCHA generation [92]	CAPTCHA based on the image is introduced along with multiple choice questions on the given set of images [95]
			Capy puzzle CAPTCHA and supervised learning for the detection of bots [90]	Amodal completion to enhance the security of CAPTCHA [96]
		Cons	-	Less work on artificial intelligence

REVIEW ARTICLE

Software widgets	Password Strength Meter	Pros	No specific work	Based on Markov Model [99]
		Cons	Automated framework missing	Automated framework missing
Security Scanner	Scanning	Pros	Security as a service	Scan web application through simulating pen tester action [103]
		Cons	Specific work not found	The performance of every scanner depends on the type of vulnerability [104]
Firewall	Different methods	Pros	firewall using packet filtering by potables [105]	firewall with an overview of models of traffic filtering [109]
	Artificial intelligence	Pros	firewall based on reinforcement learning with pattern matching [107]	An efficient firewall system is proposed by implementing KNN [110] Character level convolutions neural network is implemented [111]
		Cons	-	-

Figure 15 and Figure 16 presents the related work done in the following countries. There are ample of other countries where the research work with same parameters is done.

In Figure 15, it would be tedious to mention all countries, so only the major of them are presented in the chart. The remaining countries are Republic of China, Greece, Germany, Pakistan, Saudi Arabia, Israel, New Zealand, Australia, UAE, Malaysia, California, Kentucky, South Korea, Japan, Poland, Iraq, Egypt, Canada, Bangladesh, Nigeria, Spain, Indonesia, Russia, Bahrain, Mississippi, and France.

In Figure 16, all countries are shown in the form of a world map. The darker shade of blue implies the most relevant sources included from that specific country.

From this graph, it can be concluded that China and USA are the countries where most of the research work on the same parameters is done.

REVIEW ARTICLE

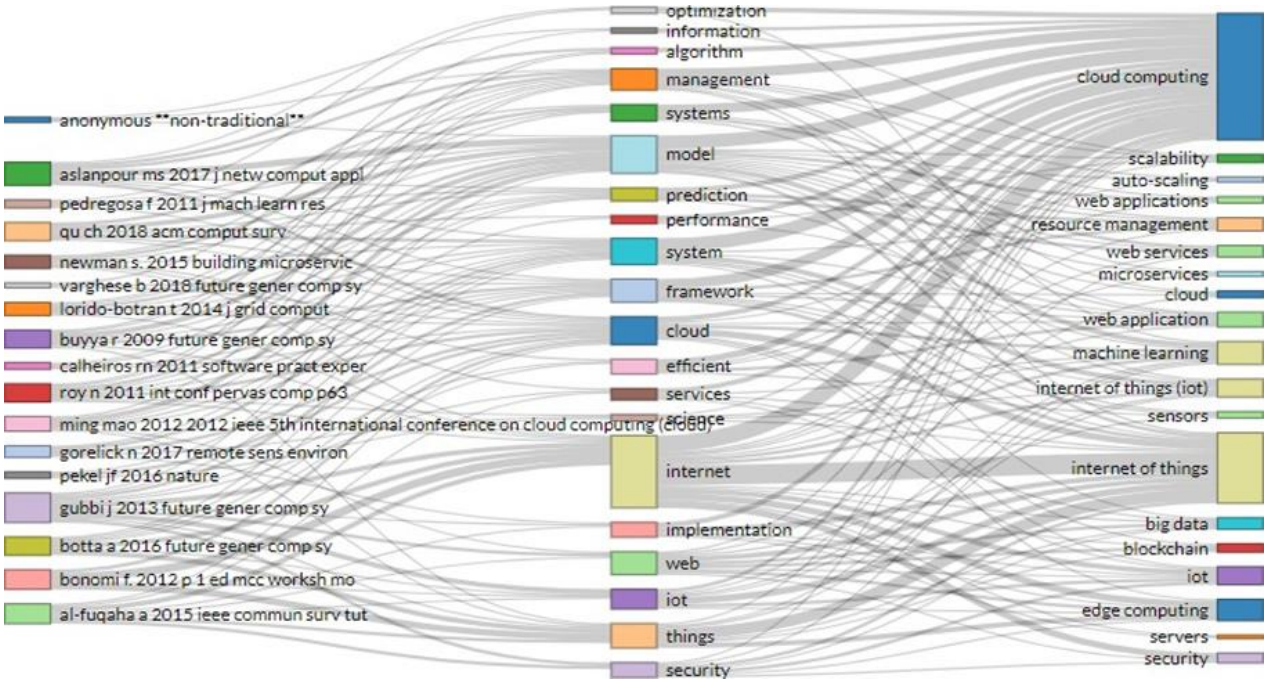

Figure 14 Three Plots Capture the Authors and Research Parameters

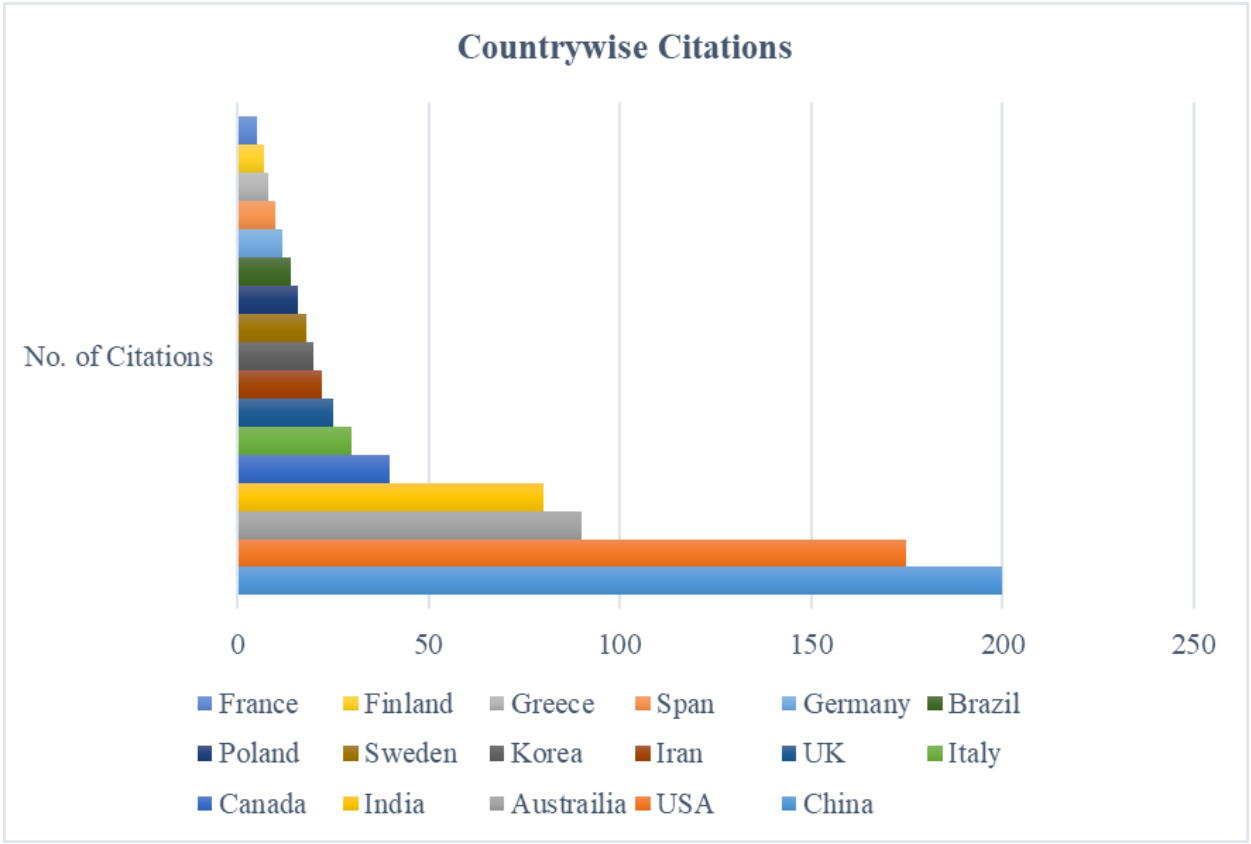

Figure 14 Country-Wise

REVIEW ARTICLE

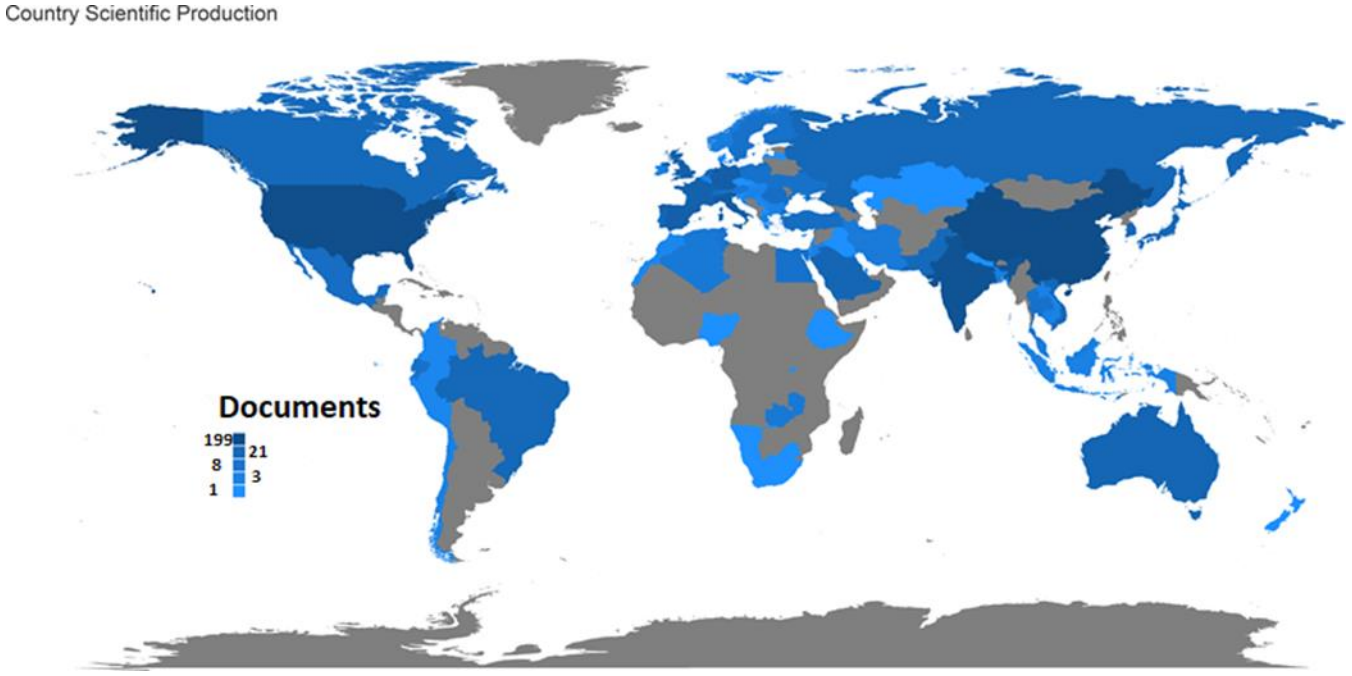

Figure 15 World Map

4. OPEN RESEARCH ISSUES AND CHALLENGES

The major objective of this study was the produce different issues and research problems for the research community. After analyzing Table 2 and Table 3 and all graphs and charts, the following research challenges have been concluded:

- Hybrid algorithms are not introduced for web-based services

Hybrid algorithms are used by the authors for enhancing security in cryptography. For web-based services, the authors proposed an advanced algorithm that combines cryptography and steganography for enhancing the security of private information [26]. A combination of RSA and other algorithms similar to this is not used in the related work.

- In the field of cryptography, for cloud-based services, most of the work combines RSA with others

because of the advantages of RSA, it is one of the widely used algorithms in public-key cryptography for reliable data transmission. Hence, it is used by many authors in hybrid algorithms. One of the authors proposes a hybrid RSA which combines two different keys, that is, the combination of a private key with the public key for encryption and decryption [38].

- In the field of cryptography, for web-based services, encryption based on passwords is not used

For web-based services, a key pair combination is not found for certificate generation. For web-based services, multi-factor authentication of digital certificates is not used. The work done for the authentication of digital certificates uses the general information of a user. The introduced certificate does not contain any public key of the user, rather than this entails birth certificate information, driving license information, etc. It is used as a secret token. Protocols based on discrete logarithm and integer factoring are used to achieve authentication [49].

- A generalized digital certificate can be implemented in the cloud too

For the authentication of digital certificates in the cloud, the most recent work implements two-factor authentication entailing biometric authentication with one-time-key [46]. The idea of using a generalized digital certificate that entails birth certificate information, driving license information, etc. No automated certificate generation framework is found for the cloud computing environment.

For a self-protection environment, more malicious attacks can be tested other than DOS and intrusion detection.

For web-based services, the authors tested a self-protection environment for DOS attack, this attack makes the website unavailable for a course of time, and for cloud-based services intrusion detection is tested. Other than DOS attacks and intrusion detection, password attack, SQL injection attack, Man in the middle attack, etc. can also be tested further.

- Mostly encryption is used for secure logging

To protect data or information from no secure access, encryption is used. This is the method that secures the data.

REVIEW ARTICLE

Therefore, it can also be used for secure logging. Signing and verifying of log data is implemented and evaluated in previous work [60]. For the logged user, the public key is implemented to validate the integrity, the secret key is used for the generation of signatures of the log. Secure logging can also be ensured by validating the user by other means.

- No robust work is introduced in web-based spam filtering

In general, spam filtering is used in emails and social networking sites. As cloud services are getting popular and widely used all over the globe, they are also prone to spam. Hence, certain authors implement spam filtering for the cloud by using certain methods and fingerprint sharing [68] [70].

- No robust system for web-based data protection

For data protection in web-based services, most recent work uses a communication system where the user needs not to communicate with each server individually. Besides, the information is communicated between the first and second servers, hence the protection data [78]. Likewise, cloud-based services implement an intelligent cryptography method through which partial data cannot be reached by cloud providers [76].

- Machine learning is not used for cloud-based password hashing and security

Machine learning is an intelligent method to train the system. It has been observed that for the security of passwords and password hashing, machine learning is not used in the previous works, which can be implemented by observing the patterns of passwords and many more.

Machine learning is less used for web-based CAPTCHA generation: For cloud-based services, the detection of bots is implemented by using supervised learning [90]. For web-based CAPTCHA generation, different methods have been used as discussed in Table 1 and Table 2. For the same, machine, learning can also be implemented.

- No specific work is done for cloud-based password strength meters and security scanning

Most passwords are used for secure logging on a web service. Hence, most web services implement password strength meters. Along with authentication, for secure logging in the cloud, password strength meters can also be implemented. Along with it, security scanning comes under security as a service only.

Spam filtering and software widgets are the least favorite topics among authors: Spam filtering and software widgets are the least favorite topics among authors who publish their work between the years 2020 to 2011.

The above observations are open research problems identified based on a systematic literature review of both cloud and web-hosting services with different security parameters. These research gaps are the need to minimize and encourage the researchers to develop some new mechanisms to provide more security to both techniques.

5. CONCLUSION

The objective of this work is to compare cloud-based and web-based services based on particular research parameters. For this, more than 250 articles have been studied out of which more than 100 papers have been cited. These papers are collected from 32 different countries. The comparison between cloud-based and web-based services is done based on eleven research parameters. These parameters are mentioned in Section 2. A detailed comparison is presented in Tables 1 and 2 and a comparative analysis of the same is provided in Section 4. This section presents the comparative analysis in the form of graphs and charts. This cannot be concluded which one is better either cloud-based service or web-based service. However, as the cloud's services and characteristics provide lots of functionality, it is the main concern and highlighted topic in the IT sector. Because of this, most researchers are interested in cloud-based services. However, few web-based services are more advanced than cloud-based. Furthermore, in the future this comparison can be done with other parameters and analysis can be made using other graphs and charts.

REFERENCES

[1] Khan, I., Dewangan, B., Meena, A., & Birthare, M. (2020, March). Study of Various Cloud Service Providers: A Comparative Analysis. In 5th International Conference on Next Generation Computing Technologies (NGCT-2019).

[2] Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of "big data" on cloud computing: Review and open research issues. Information systems, 47, 98-115.

[3] Wang, L., Ranjan, R., Chen, J., & Benatallah, B. (Eds.). (2017). Cloud computing: methodology, systems, and applications. CRC Press.

[4] Dewangan, B. K., Agarwal, A., & Pasricha, A. (2016, October). Credential and security issues of cloud service models. In 2016 2nd International Conference on Next Generation Computing Technologies (NGCT) (pp. 888-892). IEEE.

[5] Grobauer, B., Walloschek, T., & Stocker, E. (2010). Understanding cloud computing vulnerabilities. IEEE Security & privacy, 9(2), 50-57.

[6] Xu, X. (2012). From cloud computing to cloud manufacturing. Robotics and computer-integrated manufacturing, 28(1), 75-86.

[7] Kaur, M., & Singh, H. (2015). A review of cloud computing security issues. International Journal of Advances in Engineering & Technology, 8(3), 397.

[8] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation computer systems, 28(3), 583-592.

[9] Alani, M. M. (2016). Elements of cloud computing security: A survey of key practicalities. Springer International Publishing.

[10] Zahra, S., Alam, M., Javaid, Q., Wahid, A., Javaid, N., Malik, S. U. R., & Khan, M. K. (2017). Fog computing over IoT: A secure deployment and formal verification. IEEE Access, 5, 27132-27144.

[11] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. Decision support systems, 51(1), 176-189.

[12] Dewangan, B. K., Jain, A., & Choudhury, T. (2020). AP: Hybrid Task Scheduling Algorithm for Cloud. Rev. d'Intelligence Artif., 34(4), 479-485.

[13] Ashraf, M. A., Jamal, H., Khan, S. A., Ahmed, Z., & Baig, M. I. (2016). A heterogeneous service-oriented deep packet inspection and analysis framework for traffic-aware network management and

REVIEW ARTICLE

security systems. IEEE Access, 4, 5918-5936.
[14] Zou, D., Huang, Z., Yuan, B., Chen, H., & Jin, H. (2018). Solving anomalies in NFV-SDN based service function chaining composition for IoT network. IEEE Access, 6, 62286-62295.
[15] Dewangan, B. K., Agarwal, A., Venkatadri, M., & Pasricha, A. (2019). Design of self-management aware autonomic resource scheduling scheme in cloud. International Journal of Computer Information Systems and Industrial Management Applications, 11, 170-177.
[16] Bangash, Y. A., Rana, T., Abbas, H., Imran, M. A., & Khan, A. A. (2019). Incast mitigation in a data center storage cluster through a dynamic fair-share buffer policy. IEEE Access, 7, 10718-10733.
[17] Geng, R., Wang, X., & Liu, J. (2018). A software defined networking-oriented security scheme for vehicle networks. IEEE Access, 6, 58195-58203.
[18] Heartfield, R., Loukas, G., & Gan, D. (2017, June). An eye for deception: A case study in utilizing the human-as-a-security-sensor paradigm to detect zero-day semantic social engineering attacks. In 2017 IEEE 15th international conference on software engineering research, management and applications (SERA) (pp. 371-378). IEEE.
[19] Siboni, S., Sachidananda, V., Meidan, Y., Bohadana, M., Mathov, Y., Bhairav, S., & Elovici, Y. (2019). Security testbed for Internet-of-Things devices. IEEE transactions on reliability, 68(1), 23-44.
[20] Martin, W., Sarro, F., Jia, Y., Zhang, Y., & Harman, M. (2016). A survey of app store analysis for software engineering. IEEE transactions on software engineering, 43(9), 817-847.
[21] Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, 71, 28-42.
[22] Alloghani, M., & Alani, M. M. (2020). Security Challenges in Software Engineering for the Cloud: A Systematic Review. Software Engineering in the Era of Cloud Computing, 131-151.
[23] Kim, J., Kim, E., Yang, J., Jeong, J., Kim, H., Hyun, S., ... & Dunbar, L. (2020). IBCS: intent-based cloud Services for Security Applications. IEEE Communications Magazine, 58(4), 45-51.
[24] Yassin, W., Udzir, N. I., Muda, Z., Abdullah, A., & Abdullah, M. T. (2012, June). A cloud-based intrusion detection service framework. In Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) (pp. 213-218). IEEE.
[25] Chen, F., Luo, D., Xiang, T., Chen, P., Fan, J., & Truong, H. L. (2021). IoT Cloud Security Review: A Case Study Approach Using Emerging Consumer-oriented Applications. ACM Computing Surveys (CSUR), 54(4), 1-36.
[26] Chaudhary, S., Suthar, F., & Joshi, N. K. (2020). Comparative Study Between Cryptographic and Hybrid Techniques for Implementation of Security in Cloud Computing. In Performance Management of Integrated Systems and its Applications in Software Engineering (pp. 127-135). Springer, Singapore.
[27] Kumar, A., Jain, V., & Yadav, A. (2020, February). A New Approach For Security In Cloud Data Storage For Iot Applications Using Hybrid Cryptography Technique. In 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC) (pp. 514-517). IEEE.
[28] Mahalle, V. S., & Shahade, A. K. (2014, October). Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm. In 2014 International Conference on Power, Automation and Communication (INPAC) (pp. 146-149). IEEE.
[29] Sengupta, N., & Holmes, J. (2013, November). Designing of cryptography based security system for cloud computing. In 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies (pp. 52-57). IEEE.
[30] Sunitha, K., & Prashanth, S. K. (2013). Enhancing privacy in cloud service provider using cryptographic algorithm. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN, 2278-0661.
[31] Abbas, M. S., Mahdi, S. S., & Hussien, S. A. (2020, April). Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography. In 2020 International Conference on Computer Science and Software Engineering (CSASE) (pp. 123-127). IEEE.
[32] Gugnani, G., Ghrera, S. P., Gupta, P. K., Malekian, R., & Maharaj, B. T. J. (2016). Implementing DNA encryption technique in web services to embed confidentiality in cloud. In Proceedings of the Second International Conference on Computer and Communication Technologies (pp. 407-415). Springer, New Delhi.
[33] Mustacoglu, A. F., Catak, F. O., & Fox, G. C. (2020). Password-based encryption approach for securing sensitive data. Security and Privacy, 3(5), e121.
[34] Agrawal, N., & Tapaswi, S. (2019). A trustworthy agent-based encrypted access control method for mobile cloud computing environment. Pervasive and Mobile Computing, 52, 13-28.
[35] Singleton IV, L. C., & Cooper, A. (2019). U.S. Patent Application No. 16/519,243.
[36] Bhargavi, R. V., & Rao, K. N. (2015). Trusted third party framework for data security in cloud computing environment. Int J Sci Res, 4(12), 917-923.
[37] Rahmani, H., Sundararajan, E., Ali, Z. M., & Zin, A. M. (2013). Encryption as a Service (EaaS) as a Solution for Cryptography in Cloud. Procedia Technology, 11, 1202-1210.
[38] Gondaliya, J., Savani, S., Dhaduvai, V. S., & Hossain, G. (2018, April). Hybrid security RSA algorithm in application of web service. In 2018 1st International Conference on Data Intelligence and Security (ICDIS) (pp. 149-152). IEEE.
[39] Dewangan, B. K., Agarwal, A., Choudhury, T., & Pasricha, A. (2020). Cloud resource optimization system based on time and cost. International Journal of Mathematical, Engineering and Management Sciences, 5(4), 758-768.
[40] Ditta, A., Azeem, M., Naseem, S., Rana, K. G., Khan, M. A., & Iqbal, Z. (2020). A secure and size efficient algorithm to enhance data hiding capacity and security of cover text by using unicode. Journal of King Saud University-Computer and Information Sciences.
[41] Hao-yu, W., Yi, Z., & Yuan, D. (2011, March). XML-based model for data communication encryption. In 2011 3rd International Conference on Computer Research and Development (Vol. 1, pp. 258-260). IEEE.
[42] Muñoz-Gallego, A. J., & López, J. (2019). A Security Pattern for Cloud service certification.
[43] Dewangan, B. K., Agarwal, A., Venkatadri, M., & Pasricha, A. (2018). Resource scheduling in cloud: a comparative study. International Journal of Computer Sciences and Engineering, 6(8), 168-173.
[44] Manjusha, R., & Ramachandran, R. (2015). Secure authentication and access system for cloud computing auditing services using associated digital certificate. Indian Journal of Science and Technology, 8, 220.
[45] Seo, S. H., Nabeel, M., Ding, X., & Bertino, E. (2013). An efficient certificateless encryption for secure data sharing in public clouds. IEEE Transactions
[46] Chakraborty, N. R., Rahman, M. T., Rahman, M. E., & Uddin, M. S. (2016, December). Generation and verification of digital signature with two factor authentication. In 2016 International Workshop on Computational Intelligence (IWCI) (pp. 131-135). IEEE.
[47] Aas, J., Barnes, R., Case, B., Durumeric, Z., Eckersley, P., Flores-López, A., ... & Warren, B. (2019, November). Let's Encrypt: an automated certificate authority to encrypt the entire web. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 2473-2487).
[48] Le Saint, E. F. (2016). U.S. Patent No. 9,331,990. Washington, DC: U.S. Patent and Trademark Office.
[49] Harn, L., & Ren, J. (2011). Generalized digital certificate for user authentication and key establishment for secure communications. IEEE Transactions on Wireless Communications, 10(7), 2372-2379.
[50] El-Morshedy, D. S., El-Attar, N. E., Awad, W. A., & Hanafy, I. M. (2020). Trustworthy Self-protection for Data Auditing in Cloud Computing Environment. In Internet of Things—Applications and Future (pp. 23-39). Springer, Singapore.
[51] Dewangan, B. K., Agarwal, A., Venkatadri, M., & Pasricha, A. (2019). Sla-based autonomic cloud resource management framework by antlion optimization algorithm. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(4), 119-123.
[52] Lang, B., Wang, J., & Liu, Y. (2017). Achieving flexible and self-

REVIEW ARTICLE

contained data protection in cloud computing. IEEE Access, 5, 1510-1523.

[53] Baghel, S. K., & Dewangan, B. K. (2012). Defense in Depth for Data Storage in Cloud Computing. International Journal of Technology, 2(2), 58-61.

[54] Benkhelifa, E., & Welsh, T. (2014, September). Towards Malware Inspired Cloud Self-Protection. In 2014 International Conference on Cloud and Autonomic Computing (pp. 1-2). IEEE.

[55] Wailly, A., Lacoste, M., & Debar, H. (2012, September). Vespa: Multi-layered self-protection for cloud resources. In Proceedings of the 9th international conference on Autonomic computing (pp. 155-160).

[56] Yin, Z., Li, Z., & Cao, Y. (2018, June). A Web Application Runtime Application Self-protection Scheme against Script Injection Attacks. In International Conference on Cloud Computing and Security (pp. 566-577). Springer, Cham.

[57] Schmerl, B., Cámara, J., Gennari, J., Garlan, D., Casanova, P., Moreno, G. A., ... & Barnes, J. M. (2014, April). Architecture-based self-protection: composing and reasoning about denial-of-service mitigations. In Proceedings of the 2014 Symposium and Bootcamp on the Science of Security (pp. 1-12).

[58] Chen, Q., Abdelwahed, S., & Erradi, A. (2013, August). A model-based approach to self-protection in computing system. In Proceedings of the 2013 ACM Cloud and Autonomic Computing Conference (pp. 1-10).

[59] Rane, S., & Dixit, A. (2019, January). BlockSLaaS: Blockchain assisted secure logging-as-a-service for cloud forensics. In International Conference on Security & Privacy (pp. 77-88). Springer, Singapore.

[60] Lin, C. Y., Chang, M. C., Chiu, H. C., & Shyu, K. H. (2015, September). Secure logging framework integrating with cloud database. In 2015 International Carnahan Conference on Security Technology (ICCST) (pp. 13-17). IEEE.

[61] Wu, S., & Zhang, Y. (2015, October). Secure logging monitor service for cloud forensics. In 2015 IEEE 16th International Conference on Communication Technology (ICCT) (pp. 757-762). IEEE.

[62] Kunz, T., Selzer, A., & Waldmann, U. (2014). Automatic data protection certificates for cloud-services based on secure logging. In Trusted cloud computing (pp. 59-75). Springer, Cham.

[63] Ray, I., Belyaev, K., Strizhov, M., Mulamba, D., & Rajaram, M. (2013). Secure logging as a service—delegating log management to the cloud. IEEE systems journal, 7(2), 323-334.

[64] Zawoad, S., Dutta, A. K., & Hasan, R. (2013, May). SecLaaS: secure logging-as-a-service for cloud forensics. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security (pp. 219-230).

[65] Rajalakshmi, J. R., Rathinraj, M., & Braveen, M. (2014, March). Anonymizing log management process for secure logging in the cloud. In 2014 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2014] (pp. 1559-1564). IEEE.

[66] Dowling, B., Günther, F., Herath, U., & Stebila, D. (2016, September). Secure logging schemes and certificate transparency. In European Symposium on Research in Computer Security (pp. 140-158). Springer, Cham.

[67] Nesta, P. A., Zaccone, P. L., Dal Checco, P., Cavagnino, D., Bergadano, F., & Miraglia, M. (2010). U.S. Patent No. 7,770,032. Washington, DC: U.S. Patent and Trademark Office.

[68] Chen, J., Zhao, H., Yang, J., Zhang, J., Li, T., & Wang, K. (2017). An intelligent character recognition method to filter spam images on cloud. Soft Computing, 21(3), 753-763.

[69] Aun, M. T. B., Goi, B. M., & Kim, V. T. H. (2011, October). Cloud enabled spam filtering services: Challenges and opportunities. In 2011 IEEE Conference on Sustainable Utilization and Development in Engineering and Technology (STUDENT) (pp. 63-68). IEEE.

[70] Shi, W., & Xie, M. (2011, June). Spam filtering cloud platform based on sharing fingerprints. In 2011 International Conference on Computer Science and Service System (CSSS) (pp. 3570-3573). IEEE.

[71] Thomas, K., Grier, C., Ma, J., Paxson, V., & Song, D. (2011, May). Design and evaluation of a real-time url spam filtering service. In 2011 IEEE symposium on security and privacy (pp. 447-462). IEEE.

[72] Song, J., Lee, S., & Kim, J. (2011, September). Spam filtering in twitter using sender-receiver relationship. In International workshop on recent advances in intrusion detection (pp. 301-317). Springer, Berlin, Heidelberg.

[73] Odun-Ayo, I., Ajayi, O., Akanle, B., & Ahuja, R. (2017, December). An overview of data storage in cloud computing. In 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS) (pp. 29-34). IEEE.

[74] Li, J., Yao, W., Zhang, Y., Qian, H., & Han, J. (2016). Flexible and fine-grained attribute-based data storage in cloud computing. IEEE Transactions on Services Computing, 10(5), 785-796.

[75] Obrutsky, S. (2016). Cloud storage: Advantages, disadvantages and enterprise solutions for business. In Conference: EIT New Zealand.

[76] Li, Y., Gai, K., Qiu, L., Qiu, M., & Zhao, H. (2017). Intelligent cryptography approach for secure distributed big data storage in cloud computing. Information Sciences, 387, 103-115.

[77] Hu, C., Li, W., Cheng, X., Yu, J., Wang, S., & Bie, R. (2017). A secure and verifiable access control scheme for big data storage in clouds. IEEE Transactions on Big data, 4(3), 341-355.

[78] Lv, Kaili, Jian Deng, Bingyang Hua, Zengguang Liu, Chaofeng Meng, Jie Su, Jun Tang, and Zheng Zhang. "Promulgating information on websites using servers." U.S. Patent 9,401,841, issued July 26, 2016.

[79] Fanli, Z. E. N. G., Peng Lin, L. I. N. Qiqian, and W. A. N. G. Weichun. "Method of storing data and data storage managing server." U.S. Patent 10,001,945, issued June 19, 2018.

[80] Madabattula, S. Y. A., & Madira, S. R. R. (2020). Secured Authentication With One Time Password on the Cloud.

[81] Xylogiannopoulos, K. F., Karampelas, P., & Alhajj, R. (2020). A password creation and validation system for social media platforms based on big data analytics. Journal of Ambient Intelligence and Humanized Computing, 11(1), 53-73.

[82] Kamal, P. (2019). Security of Password Hashing in Cloud. Journal of Information Security, 10(02), 45.

[83] Ayankoya, F., & Ohwo, B. (2019). Brute-force attack prevention in cloud computing using one-time password and cryptographic hash function. International Journal of Computer Science and Information Security (IJCSIS), 17(2).

[84] Billa, J. B., Nawar, A., Shakil, M. M. H., & Das, A. K. (2019, June). PassMan: A new approach of password generation and management without storing. In 2019 7th International Conference on Smart Computing & Communications (ICSCC) (pp. 1-5). IEEE.

[85] Chari, Suresh, Taesung Lee, Ian Michael Molloy, and Youngja Park. "Two-level sequence learning for analyzing, metering, generating, and cracking passwords." U.S. Patent 10,609,017, issued March 31, 2020.

[86] Ntantogian, C., Malliaros, S., & Xenakis, C. (2019). Evaluation of password hashing schemes in open source web platforms. Computers & Security, 84, 206-224.

[87] Jeong, J., Woo, D., & Cha, Y. (2019, December). Enhancement of website password security by using access log-based salt. In 2019 International Conference on Systems of Collaboration Big Data, Internet of Things & Security (SysCoBIoTS) (pp. 1-3). IEEE.

[88] Seta, H., Wati, T., & Kusuma, I. C. (2019, October). Implement time based one time password and secure hash algorithm 1 for security of website login authentication. In 2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS) (pp. 115-120). IEEE.

[89] Ogiela, U. (2020). Cognitive cryptography for data security in cloud computing. Concurrency and Computation: Practice and Experience, 32(18), e5557.

[90] Arai, T., Okabe, Y., Matsumoto, Y., & Kawamura, K. (2020, January). Detection of bots in captcha as a cloud service utilizing machine learning. In 2020 International conference on information networking (ICOIN) (pp. 584-589). IEEE.

[91] Althamary, I. A., & El-Alfy, E. S. M. (2017, May). A more secure scheme for CAPTCHA-based authentication in cloud environment. In

REVIEW ARTICLE

2017 8th International Conference on Information Technology (ICIT) (pp. 405-411). IEEE.
[92] Shumilov, A., & Philippovich, A. (2016, January). Cloud-based CAPTCHA service. In 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence) (pp. 115-118). IEEE.
[93] Saxena, A., Chauhan, N. S., Kumar, S., Vangal, A. S., & Rodrguez, D. P. (2012, October). A new scheme for mobile based CAPTCHA service on Cloud. In 2012 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM) (pp. 1-6). IEEE.
[94] Vaithyasubramanian, S., Lalitha, D., & Kirubhashankar, C. K. (2019). Enhancing website security against bots, spam and web attacks using l CAPTCHA. International Journal of Computers and Applications, 1-7.
[95] Das, M., Naresh, A., Narang, A., Narayana, A., & Jayashree, R. (2016, December). Automated CAPTCHA Generation from Annotated Images Using Encoder Decoder Architecture. In 2016 International Conference on Information Technology (ICIT) (pp. 45-50). IEEE.
[96] Azakami, T., & Uda, R. (2017, March). Deep Learning Analysis of Amodal Completion CAPTCHA with Colors and Hidden Positions. In 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA) (pp. 341-346). IEEE.
[97] Torky, M., Meligy, A., & Ibrahim, H. (2016, December). Securing Online Social Networks against bad Bots based on a Necklace CAPTCHA approach. In 2016 12th International Computer Engineering Conference (ICENCO) (pp. 158-163). IEEE.
[98] Yang, Y., Yeo, K. C., Azam, S., Karim, A., Ahammad, R., & Mahmud, R. (2020, June). Empirical Study of Password Strength Meter Design. In 2020 5th International Conference on Communication and Electronics Systems (ICCES) (pp. 436-442). IEEE.
[99] Bodkhe, U., Chaklasiya, J., Shah, P., Tanwar, S., & Vora, M. (2020). Markov model for password attack prevention. In Proceedings of first international conference on computing, communications, and cyber-security (IC4S 2019) (pp. 831-843). Springer, Singapore.
[100] Sahin, C. S., Lychev, R. D., & Wagner, N. (2020). U.S. Patent No. 10,546,116. Washington, DC: U.S. Patent and Trademark Office.
[101] Murray, A., Begna, G., Nwafor, E., Blackstone, J., & Patterson, W. (2015, April). Cloud service security & application vulnerability. In SoutheastCon 2015 (pp. 1-8). IEEE.
[102] Andrian, R., & Fauzi, A. (2020). Security scanner for web applications case study: Learning management system. Jurnal Online Informatika, 4(2), 63-68.
[103] Seng, L. K., Ithnin, N., & Said, S. Z. M. (2018). The approaches to quantify web application security scanners quality: a review. International Journal of Advanced Computer Research, 8(38), 285-312.
[104] Idrissi, S. E., Berbiche, N., Guerouate, F., & Shibi, M. (2017). Performance evaluation of web application security scanners for prevention and protection against vulnerabilities. International Journal of Applied Engineering Research, 12(21), 11068-11076.
[105] Hempfling, C. (2017). A Packet-Filtering Firewall for Cloud Computing. Department of Computer Science-Chair of Computer Science II-Julius-Maximilians-University.
[106] Dezhabad, N., & Sharifian, S. (2018). Learning-based dynamic scalable load-balanced firewall as a service in network function-virtualized cloud computing environments. The Journal of Supercomputing, 74(7), 3329-3358.
[107] Praise, J. J., Raj, R. J. S., & Benifa, J. B. (2020). Development of Reinforcement Learning and Pattern Matching (RLPM) Based Firewall for Secured Cloud Infrastructure. Wireless Personal Communications, 115(2), 993-1018.
[108] Diovu, R. C., & Agee, J. T. (2017, June). A cloud-based openflow firewall for mitigation against DDoS attacks in smart grid AMI networks. In 2017 IEEE PES PowerAfrica (pp. 28-33). IEEE. Clincy, V., & Shahriar, H. (2018, July). Web application firewall: Network security models and configuration. In 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC) (Vol. 1, pp. 835-836). IEEE.
[109] Sahin, M., & Sogukpınar, I. (2017, October). An efficient firewall for web applications (EFWA). In 2017 International Conference on Computer Science and Engineering (UBMK) (pp. 1150-1155). IEEE.
[110] Ito, M., & Iyatomi, H. (2018, March). Web application firewall using character-level convolutional neural network. In 2018 IEEE 14th International Colloquium on Signal Processing & Its Applications (CSPA) (pp. 103-106). IEEE.
[111] Molnar, D., & Schechter, S. E. (2010, June). Self Hosting vs. Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud. In WEIS.
[112] Dewangan, B. K., Venkatadri, M., Agarwal, A., Pasricha, A., & Choudhury, T. (2021). An Automated Self-Healing Cloud Computing Framework for Resource Scheduling. International Journal of Grid and High Performance Computing (IJGHPC), 13(1), 47-64.
[113] Lorenc, P., & Woda, M. (2017). IaaS vs. Traditional Hosting for Web Applications-Cost Effectiveness Analysis for a Local Market. In Advances in Dependability Engineering of Complex Systems (pp. 233-243). Springer, Cham.
[114] Dewangan, B. K., Agarwal, A., Venkatadri, M., & Pasricha, A. Macro: Cost-Oriented Autonomic Resource Management for Cloud Computing. Vivekananda Journal of Research, 106.

Authors

Dr. Bhupesh Kumar Dewangan pursued Ph.D. in computer science and engineering and working as an Associate Professor in the Department of Computer Science and Engineering, at the OP Jindal University Raigarh, India, Bachelor of Technology from Pandit Ravi Shankar Shukla University (STATE UNIVERSITY), Raipur and Master of Technology from Chhattisgarh Swami Vivekananda Technical University (STATE TECHNICAL UNIVERSITY), Bhilai in computer science and engineering. He has more than 40 research publications in various international journals and conferences with SCI/SCOPUS/UGC indexing. He has three Indian patents on Cloud computing and resource scheduling. His research interests are in Autonomic Cloud Computing, Resource Scheduling, Software Engineering, and Testing, Image processing, and Object detection. He is a member of various organizations like ISTE, IAPFE, etc. Currently, he is editor in special issue journals of Inderscience & IGI publication house, and editor/author of two books of Springer & Taylor and Francis publication house.

Dr. Piyush Chauhan is currently working as an Associate Professor and Examination In-charge at Symbiosis Institute of Technology, Nagpur Campus. With a Ph.D. in Computer Science and Engineering, his research interests include machine learning, data analytics, smart healthcare systems, and human–computer interaction. He has prior experience in both academia and industry and has contributed to various funded projects and scholarly publications.

How to cite this article:

Bhupesh Kumar Dewangan, Piyush Chauhan, "An Extensive Review of Hosting of Cloud, IoT, and Web-Based Services: Security Issues and Challenges Ahead", International Journal of Computer Networks and Applications (IJCNA), 12(3), PP: 363-383, 2025, DOI: 10.22247/ijcna/2025/23.