Analysis of Cloud and Self-Web-Hosting Services Based on Security Parameters

Surbhi Khare, Department of CSE, MATS School of Engineering, India & IT MATS University, Raipur, India*
Abhishek Badholia, Department of CSE, MATS School of Engineering, India & IT MATS University, Raipur, India

ABSTRACT

Most of the web applications are hosted by cloud due to low cost and low infrastructure setup required. In this paper, the technology, self web hosting, and cloud web hosting are compared based on different security parameters like key generation (PKI), automatic authentication and protection of intra-tenant networks, secure logging system events, spam filtering, CAPTCHA generation and authentication, and software widgets such as password metering. These parameters are classified into seven categories, and the review has been conducted based on these categories. The bibliometric analysis has been conducted with more than 70 studies found in Web of Science (WoS) database through bibliometric library and biblioshine package in R programming. The outcome of this analysis is presented in tabular form, and open challenges of both the technologies are discussed in detail with proposed solutions.

KEYWORDS
Authentication, Captcha, Certificate and Public/Private Key Generation, Cloud, Password Hashing, Security

INTRODUCTION

The objective of this paper is to provide an extensive comparative analysis between self-web-hosting and cloud-web-hosting techniques based on security parameters.

Self-Web-Hosting

Web hosting is an internet service that allows big organizations and individuals to post a website or web page onto the Internet. Many kinds of websites are hosted and stored are on special computers called servers. When customers/users want to access your website, they just requires to do is write your website address or domain into their browser. Their PC will then be able to connect to your server and the webpages will be accessible to them through the browser (Martin, J., 2021).

Various kinds of web hosting are available depending on business needs, budget, and what kind of resources the web host offers. There are Website Builders, Shared Hosting, Dedicated Hosting, and Collocated Hosting.

A website builder is for beginners whose services mainly provide the user with an online browser-based interface to build their website and host the website for the user without any additional setup.
Collocated hosting means that users/organization can purchase their server and have it housed at a web host’s facilities. It gives users/organizations full control over web server resources so as now they don’t need to share their resources with others. They can install any scripts or applications they need. It’s quite expensive but some companies can use it for faster output (Valentine, T., 2021).

Shared hosting means individual users and other website owners have to share one server for resources. It is the most commonly used hosting opted by many companies as these services are affordable because the cost to operate a server is shared now between the user and the other owners.

In dedicated hosting, users have the entire web server to itself which allows faster performance, as the user can now have all the server’s resources without sharing with other website owners. However, it also means that the user will be responsible for the cost of server operations entirely. This is a very good choice for websites that need a lot of system resources or require a higher level of security.

To distribute your website onto the web, your business website requires a web hosting administration. If we look at it this way, the web has given entrepreneurs something beyond web hosting administrations. For instance, web hosting firms regularly utilize in-house professionals to ensure their customers’ sites are ready for action every minute of every day. Furthermore, when site proprietors are needing assistance or investigating (for example script debugging, email not ready to send/get, area name reestablishment, and that’s just the beginning), the web host’s in-house support is the go-to individuals.

An expert web hosting (as shown in Figure 1) administration guarantees an issue-free encounter for entrepreneurs, so they can productively zero in their time and exertion on their organizations.

**Cloud-Web-Hosting**

Cloud hosting illustrates storage allocated in virtual space. Rather than purchasing a fixed space on the server, the user now needs to pay only for the resources being used. It is relatively fresh compared with an older version, which has been in existence for many years now and is understood by its functioning for users (Jain, A., & Choudhury, T., 2020). Cloud hosting is a type of web hosting which utilizes multiple servers to adjust the load and maximize uptime. Rather than utilizing a single server, your site can take advantage of the cluster that utilizes assets from an incorporated pool. This implies that regardless of whether one server fails, another kicks in to keep everything running. Cloud hosting can somewhat help in overcoming the challenges faced in web hosting like the problem of recurring downtime can be solved as if one server fails, another kicks in to minimize downtime. It also helps in reducing security risks as it consists of a dedicated IP address.

The structure of the review follows as an introduction to the background, related work, research issues and challenges, and possible solutions and conclusions.
RELATED WORK

The previous research work is classified into seven categories based on the dataset considered from Web-of-Science (WoS) website. In this, articles published from 2011 to 2021 have been considered. The related research work is described as follows:

Public/private Key Generation, Certificate Generation, and Storage

In this category, a total of 1459 research articles were found in the WoS database from the beginning of the research to date. For this, 500 out of 1459 research articles are considered for bibliometric analysis through R programming. To continue to this, the database is classified into three field plots based on author and publication details, keywords, and the name of the country where the research has been conducted. Most of the research done in this category belongs to the 1970s to 2000s. Mostly china leads the major research issue in encryption and cryptography techniques. Figure 2 presents three field plots for research done to the date of key/certificate generation by related keywords and countries mapped with authors and year of publications.

Out of 1459 research which considered this category, some research work and their contributions are as follows.

Authors Yunakovsky, S. E., et al., proposed a system, in which they find the attacks in quantum computing through public-key infrastructure. They have successfully identified the attacks and secured quantum computing in fast transition (Yunakovsky, S. E., et al., 2021), where authors Ma, M. et al., presented a novel approach to secure cloud through certificates method by applying public key generation technique. This research is based on searchable encryption methods to secure the system (Ma, M. et al., 2020). Authors Li, J. et al., presented multi-recipient key generation techniques to secure IoT-enabled applications in the cloud. In this, they can protect the system through different threats, where Xu, Z., et al., approaches for certificates signature scheme named CLAS, which is mainly based on private key generation (Authors Li, J. et al., 2018), before this, Ma, S. proposed a system which is public-key based setting equijoin system to protect multiple data flow I by contributors (Ma, S., 2017).

Figure 2. Three field plots for research done till the date of key/certificate generation by related keywords and countries mapped with authors and year of publications.
Automatic Authentication and Protection of Intra-Tenant Network Communications

Most of the research based on automatic authentication in the intra-tenant network is conducted in China and the USA. The most common keywords used in this research area are protection, relay-protection, distance-protection, and integrity-protection, whereas, in India, most of all keywords are taken into considerations to research this area.

Out of 2000 research that considered this category, and three field plot has been generated through R programming for further analysis and presented in Figure 3. Some research work and their contributions are as follows.

Vleju, M. B. presented an automatic authentication technique for cloud-based solutions. In this, the author implemented a client identity management system through which only authenticated users can have permission for accessing the applications (Vleju, M. B., 2014).

Leitold, F., proposed an anti-malware system to protect the office-365 cloud. Authors can protect cloud-based office-365 applications like share-point, one drive which protects from malware binaries and malicious hyperlinks (Leitold, F. et al., 2017).

Mann, Z. Á., et al., presented a system named RADAR, for protecting the cloud/fog application during run time through a data protection scheme by RADAR (Mann, Z. Á., et al., 2021).

Layec, P., proposed restoration and protection methods for fiber optical in networks. In this, they introduce a novel approach to protect optical networks by cuts with bandwidth variations (Layec, P., et al., 2018).

Ma, X., presented a reversible privacy-protection method to secure cloud video inspections. In this, authors also keep all records of non-privacy data which leads the no losses of information (Ma, X., et al., 2015).

Secure (Append-Only) Logging of System Events

In this research area, only 35 research are found in the WoS dataset, based on this tree plot is generated through R programming and bibliometric library through biblioshine package and presented in Figure 3. Three field plots for research done till the date of automatic authentication and protection in intra-tenant network communications by related keywords and countries mapped with authors.
Figure 4 for analysis. Based on the Tree plot, the most commonly used keyword is security, and then privacy, efficiency, and internet come. Out of 35 research, some of the research contributions are discussed as follows.

Lee, S., et al., presented a system POSTER, which describes that how the user can secure their logs. In this, they have proposed a backward/forward secrecy-based to the ARM TrustZone to secure the embedded system (Lee, S., et al., 2019).

Karande, V., et al., presented the Sgx-log system which is ensured to maintain the confidentiality and integrity of log data over Ubuntu 14.04. Sgx-log can protect the disk and memory from unauthorized access (Karande, V., et al., 2017).

Koumidis, K., et al., presented a real-time secured cyber-physical model to secure the blocks of each level in blockchain techniques. This model is based on optimizing different resources over blockchain technology (Koumidis, K., et al., 2019).

Tian, H., et al., presented a model which ensures security over the cloud by using blockchain technology. They have produced an efficient and secured public auditing method for user behaviors (Tian, H., et al., 2020).

Rane, S., et al., produce a vector-based model which ensures to protect the system from malicious attacks from malware which is mainly focused to destroy the user log data (Rane, S., 2020).

Spam Filtering

Villasenor, S., et al., Machine-learning techniques for green and powerful Web-tables junk mail filtering that become examined on a huge scalable Web-tables aggregation of approx. 36 million tables to used (Villasenor, S., et al., 2017).

Bosaeed, S., et al., presented a device to discover junk mail from messages, even though the paintings may be implemented to each incoming/outgoing SMS. They expand a device that incorporates a couple of machine-learning (ML) primarily based classifiers constructed through the use of 3 type techniques -- NB, SVM NBM. The device is constructed to permit its computation in cloud/fog or part layers. The device detects junk mail SMSs and offers pointers at the junk mail classifiers and filters for use primarily based totally on person alternatives which include type accuracy (Bosaeed, S., et al., 2020).

Figure 4. Tree plot for research done till the date of secure logging in cloud hosting services by related keywords plus
Password Hashing and Storage

Password hashing and storage techniques are the most commonly use techniques to secure any web/cloud application. Total 93 research work which is combined both the above-mentioned technique, these research works are downloaded from WoS database and applied R programming to plot word growth chart and presented in Figure 5. The analysis says that protocol attacks were highly found around 2017, where password authentication techniques are widely used nowadays. Some of the related works are discussed as follows.

Zeidler, C., and Asghar, M. R. presented a secured system AuthStore, which is based on server authentication to the cloud data. In this, they have proposed a system through which users can reuse the password in an encrypted format to secure their credentials over the cloud (Zeidler, C., & Asghar, M. R., 2018).

Patil, S., presented a password management model which is based on pen-drive to secure online accounts. In this, authors save the password into pen-drive, the credentials are nowhere else submitted apart from pen-drive (Patil, S., et al., 2019).

Vasco, et al., proposed the APAKE model, which is based on password-authentication and key-exchange protocol. Through this, no one has the client information to access their credential, and APAKE is efficient to secure the client’s credentials from unauthorized access (Vasco, et al., 2019).

Song, H., et al., presented a model through which they can secure the cloud storage, this mechanism is based on data encryption and dispersions (Song, H. et al., 2021).

CAPTCHA Generation and Verification

Ouyang, Z., et al., presented a multi-viewed stacking model based on CAPTCHA over cloud applications. In this, they proposed an indigenous technical knowledge ITK-training learning algorithm that reduces the deployment cost and time as well (Ouyang, Z., et al., 2021).

Ogiela, L., et al., proposed a technique of protection of visible data, committed to carrier control. These techniques are very crucial in protection. The main thoughts are primarily based totally on visible captcha strategies. Application of visible captcha strategies can be offered in particular inside the context of carrier control inside the Cloud. This system of offerings control inside the cloud and helps control procedures and secure offerings with the aid of using the use of visible codes procedures (Ogiela, L., et al., 2017).

Figure 5. The word growth chart for password hashing and storage research work through R programming bibliometric library.
Arai, T., et al., used the supervised learning model to generate CAPTCHA and secure the logging system. They consciousness a unique model that is Capy-puzzle to generate a CAPTCHA, that’s extensively utilized in business service. This system gains knowledge of methods to discover bots (Arai, T., et al., 2020).

In 2018, Guerra, M., et al., presented disappearance CAPTCHA, a method that, leveraging relied on different sensors in a stable detail positioned on a cellphone can isolate people from computer systems in a manner this is obvious to users (Guerar, M., et al., 2018). In continue to this, author Ravi, N. C. et al., developed of getting entry to manipulate methods has been created to layout stable digital pockets primarily based totally system. The essential issues concerning pockets protection were discussed. These methods are usually applied in the case of economic sectors. The cost of a person is typically represented in virtual pockets and protection of such virtual pockets is mandatory. To increase the protection of such virtual E-wallets this study has delivered many protection strategies which are session primarily based on total protection (Ravi, N. C. et al., 2018).

Software Widgets Such as Password-Strength Meters
Jones, M. D., et al., presented PHUI-kit to secure the system through software widgets like password metering process (Jones, M. D., et al., 2018) whereas Vázquez, D. E., et al., presented software widgets based on GUI which secure the mobile applications (Vázquez, D. E., et al., 2018).

Comparison Between Self-Hosted Web and Cloud-Hosted Web Allocation
Cloud hosting and web hosting are different from each other in many aspects. Both of them have a lot of advantages & depending on the needs, each of one of them has its application. Below are some aspects which determine which is better in what sense. The comparative analysis is done between both self and cloud-hosted web applications in different parameters and presented in Table 1.

ISSUES AND OPEN RESEARCH PROBLEMS
The self-hosted web and cloud-hosted web applications are studied and compared on different parameters and the following issues are the outcomes of this review.

Challenges in Self-Hosted Web Applications and Possible Solutions

Slow Website Loading and Navigation Speed
Companies pay a heavy load for slow loading websites as it makes gives a really bad user experience. Users hardly return to a website that takes a long time to load or has very slowly into internal navigation. Almost it is like three out of every four web users will not and never return to this kind of website which takes more than three seconds to load. Because of this, poorly time of page load time affects the Google ratings badly and negatively, leading to a decrement reputation of the company.

Solutions
1. Locating all the servers across the globe. The location of the data center that hosts the website makes the page load time of the website less notable way.
2. Utilization of extremely top-notch equipment and infra will help in lessening network inactivity to an incredible degree. Organization idleness implies time taken for a piece of information to reach starting with one point then onto the next point.
3. Giving Content Delivery Network (CDN) will make accessible stored variants of the static segments of the site at advanced rates, to a few areas.
The Challenge of Maintaining Uptime

Web facilitating thrives in a profoundly temperamental environment. Workers going down and different difficulties are normal. However, the vacation of the site is deadly in the web facilitating industry, and can even prompt the passing chime of the customer’s business. Web facilitating associations need to ensure 99.9% least uptime rate, which is as per industry standard. If it’s more than around 10 minutes of personal time seven days is grievous. The fundamental purposes behind spontaneous, crisis vacation are inaccessibility of burden balancers, equipment or programming disappointment,

| Parameters  | Self-hosted web                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Cloud-hosted web                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Control     | Web hosting is limited with space and power. Also, it can be provided to one or several clients. As a rule, at the beginner stages, websites give more preference to shared hosting. It is more cost-effective, and the company providing resources is responsible for the management, support, and security. This deducts part of the work from the owner’s end and does not require deep knowledge in this area.                                                                 | Due to the availability of several virtualized servers that are synchronized, cloud hosting allows for load balancing.                                                                                                                                                                                                                                                                                                                                                                                                               |
| Resource    | In most cases, companies offering web hosting services provide additional services as well. It can be automatic backups, or free domain registration, and much more. This enables a beginner internet entrepreneur to fast receive the required additions to the website and launch his web resources asap (Dewangan B.K. et al., 2020).                                                                 | Cloud hosting offers the client root access to the control panel and assists in disaster recovery are required. Moreover, in case of bugs, the user can switch to another server and resume working.                                                                                                                                                                                                                                                                                                                                                   |
| Scalability | Over time, the user may want to scale his website. Using conventional hosting, when there are not enough resources, has two options for events. Users are changing their plan or service provider. Now, cloud hosting has more flexibility in this. To scale, it does not require a server restart, and this can be done at any time.                                                                 | The distribution of resources can take place as quickly as possible, and there is no requirement to wait, as it is in the case of web hosting. A flexible payment system allows you not to overpay, and free up unwanted space. In the end, companies often overpay for unutilized resources by choosing a hosting web service. Users can connect any additional resources that they need in the cloud, be it RAM or network bandwidth. This will take just a few clicks. The site owner decides when he needs how many resources and pays only for what he uses. |
| Security    | Reliable web hosting service providers safeguard your server from malicious activity. They safeguard against data hacking, giving access to customers to keep their information confidential. Security measures include automatic scanning of all the programs for viruses, SSL certificates, various plug-ins, and safeguarding against spammers and viruses. | Despite the high and effective reliability of conventional web hosting providers, the cloud in many ways can bypass them. It is a safer way to store the data. The above security methods can be complemented by installing web application firewalls and advanced monitoring systems (Dewangan B.K et al., 2019).                                                                                       |
| Cost        | Cost is varied from provider to provider. However, the fact remains constant that when you purchase conventional web hosting, users purchase for fixed resources.                                                                                                                                                                                                                                                                                                                                                                                                                         | But in the case of cloud hosting, the user only pays for the utilized resources. Which is more profitable depends on what you need (Agarwal A. et al., 2018).                                                                                                                                                                                                                                                                                                                                 |

The Challenge of Maintaining Uptime

Web facilitating thrives in a profoundly temperamental environment. Workers going down and different difficulties are normal. However, the vacation of the site is deadly in the web facilitating industry, and can even prompt the passing chime of the customer’s business. Web facilitating associations need to ensure 99.9% least uptime rate, which is as per industry standard. If it’s more than around 10 minutes of personal time seven days is grievous. The fundamental purposes behind spontaneous, crisis vacation are inaccessibility of burden balancers, equipment or programming disappointment,
security penetrates, and manager blunders. Arranged personal time, for unavoidable support, is best performed at off-top hours when the site see tally is for the most part at its least.

Solutions
1. Deploying stable programming, and consistently update, to forestall programming disappointment.
2. Sending great quality and demonstrated equipment foundation.
3. Undertaking intermittent programming and equipment review for pre-empting oldness.
4. Giving 24x7 premise online help customers to determine customer questions and issues.
5. Giving FAQs, client discussions, and different gatherings to share information, for quick unravel of issues, and surprisingly pre-empt issues through opportune customer activity.
6. Confirming sound organization security check
7. Checking sufficient insurance from risks, for example, floods and fire at the found server farms.

Challenges of Providing Scalability
The present online business organizations and site proprietors anticipate exceptionally versatile assets. Be that as it may, facilitating suppliers are regularly unable to offer it. Most web facilitating organizations experience the ill effects of obsolete frameworks, similar to old worker equipment, obsolete programming, a limited broadband association, and inappropriately gifted care staff. Such limitation forced an asset crunch, which confines versatility. In any event, when it isn’t a lot of amiss with the product or equipment, the restricted assets being conveyed or the engineering of the server farm may make bottlenecks. Arising specialists like IoT, Artificial Intelligence, and Big Data offer unbound potential outcomes and huge requests on assets. The failure to scale the assets in the future may prompt sites ricocheting because of some obscure limitations, powerlessness to get to the letter drop or send email connections, and cut-off points being forced with no decision to moderate it. For customers, this influences botched freedoms and the helpless end-client experience.

Solutions
1. Overhaul their heritage framework now and again to check they give to fulfill the needs made by emerging advances.
2. Detect the hole among prerequisites and framework capacities and make up for the shortfall by provisioning the required equipment and programming.
3. By overhauling staff abilities through preparing and different mediations to guarantee that they are adequately able to do the needful when required

Security Challenges
Web facilitating organizations are consistently under steady dread of safety. Digital penetrates are the overall thing to take care of. Penetrates are deadly as far as loss of touchy information, devastating administrative fines, loss of trust, notoriety, and significantly more. A typical trap from web facilitating specialist co-ops is missing to block URL access. Without such reductions, unapproved clients may see pages that are confined to them. With such empowered admittance, assailants may effectively fashion URLs to get covered up pages. Most web facilitating specialist co-ops offer shared facilitating as a financially savvy answer for customers. Be that as it may, giving out an IP address among customers implies connecting separate areas utilizing a solitary worker. At the point when a customer is a blocklist as a spammer, it might prompt a circumstance where any remaining customers having a similar IP will likewise block the list.

Solutions
1. Deploy the most recent and confirmed security foundation, similar to firewalls, organizing checking frameworks, and that’s only the tip of the iceberg.
2. Implement the Secure File Transfer Protocol (STFP) to plug escape clauses.
3. Blocking all document types not served by the application.
4. Create an entrance control lattice that prevents unapproved clients from reviewing content.
5. Implementing exacting access control components at the server farm forestalls maverick insiders and unapproved aggressors from assuming actual responsibility for basic web resources.

Challenges in Cloud-Hosted Web Applications and Possible Solutions

Optimizing Cloud Expenses

It’s perhaps the most difficult occupation for cloud clients. A fairly more than security issues, overseeing cloud spending is an extreme assignment. With various reasons included, associations will in general waste a considerable amount of their financial plan on pointless exercises required through the cloud. Be it inconsiderateness, absence of information, rushed tasks, untalented assets – what happens is that the expenses related to distributed computing go past limits.

Solutions
1. Seeking help from different innovative answers for cloud cost the executives.
2. Involving a distributed computing accomplice who is gifted and experienced at cloud arrangement the executives.
3. Creating an incorporated cloud group to take a gander at the spending subtleties.

Working With Poly Cloud Environments

With expanding alternatives in cloud arrangements, most ventures are moving towards the multi-cloud model of working. This procedure carries alongside it numerous cloud types just as various cloud merchants included. That itself represents a test to deal with the synchronization, security, and heartiness of activities inside the association just as with various cloud specialist organizations.

Solutions
1. Applying compelling practices like doing research and preparing.
2. Dynamically overseeing vendor connections.
3. Reshaping cycles to include more partners and cloud designs.
4. Integrating cloud arrangements by different specialist co-ops into one.
5. Managing and keeping a legitimate framework to incorporate the whole working.

Migration of Existing Applications onto the Cloud

The client analyzes fostering a new cloud application as against moving a current application onto the cloud – the appropriate response is straight and straightforward. Moving a current one has its arrangement of obstacles, disadvantages, and difficulties to confront. Time has demonstrated that cloud relocation experiences confronted difficulties like security arrangement, time utilization, spending flood, unequaled prerequisites, vacation, and so forth (Agarwal, A. et al., 2019).

Solutions
1. Performing pre-relocation testing that centers basically around movement-related necessities.
2. Setting a reasonable task cut-off time and spending remembering relocation bothers.
3. Hiring cloud specialist co-ops who are specialists at movement projects.

Adapting the Cloud-first Model

Numerous undertakings aren’t yet set up to accept the cloud culture however are as yet surging onto doing it, given friend contest on the lookout. It strikes as an abnormal situation for such associations who don’t comprehend the total meaning of the cloud and have half information on how precisely
the cloud would help their business. They can’t comprehend the progressions in tasks, foundation, and climate that would be available with distributed computing arrangements.

Solutions
1. Training associations with much-required information about the cloud.
2. Appraising groups about what is available for them, after cloud execution.
3. Showing them live examples of overcoming adversity that has profited out of cloud executions.

Cost Calculations Within Limits
Since cloud activities are nearly new, associations don’t will in general spending plan their costs appropriately. Operational expenses may contrast venture to big business and the spending plan may vary. There could be some concealed costs that may will in general change as far as possible and get over. Indeed, even private ventures think that it’s hard to execute cloud arrangements inside the specified spending plan.

Solutions
1. Preparing a quote plan directly all along.
2. Involving cost specialists who can predict all included use.
3. Keeping to the side a segment of the financial plan for concealed circumstances.

Converting Back Office Activities
It is simple for the improvement culture to relocate to the cloud alongside their innovative headways. Concerning the backend measures like bookkeeping and charging frameworks have an intense errand with the changeover since they will move more towards a membership arranged arrangement. This could hamper group repayment, participation information, and so on.

Solutions
1. Maintaining all fundamental representative data in the cloud directly all along.
2. Having a definite way to deal with moving bookkeeping and account subtleties to the cloud.

Meeting Governing Compliance
Since the cloud offers benefits in mass, they are consistently popular and that’s only the tip of the iceberg so is the information preparing across cloud arrangements. The superb concern, accordingly, is the security of the data that is being prepared. Ensuring this information is the duty of the cloud specialist co-op just like the customer. Keeping rules and guidelines is essential to guarantee the exactness and security of the data stream in the cloud.

Solutions
1. Designing consistency conventions in security structures.
2. Being more focused on information flow and important security.
3. Implementing a cloud the board arrangement that sticks to administrative consistency for most extreme information security.

CONCLUSION
This paper is mainly focused on findings of self-web-hosting and cloud-web-hosting techniques proposed by many researchers from the beginning to date. The related research is taken from the WoS database by using many search keys based on different security parameters. The observations of the analysis were conducted to prove that many research challenges are still open to overcome
for better security and trust over the internet applications. The database downloaded from WoS is classified into seven different categories and the bibliometric analysis is conducted on different levels and plots like three field plots, Word tree, and Tree of keywords depending upon the number of research varies from 70 or above. The different self-web-hosting challenges like Slow Website Loading and Navigation Speed, The Challenge of Maintaining Uptime, Challenges of Providing Scalability, Security Challenges are identified. Whereas in cloud-web-hosting, Optimizing Cloud Expenses, Working with Poly Cloud Environments, Migration of Existing Applications onto the Cloud, Adapting the Cloud-first Model, Cost Calculations within Limits, Converting Back Office Activities, and Meeting Governing Compliance. To continue to this, the proposed solutions are also discussed where each challenge is presented. As per the analysis, we recommend a cloud-based web-hosting service. Moreover, the inclusion of all research is not possible to mention in this article, the selected articles were discussed and analyzed based on different security parameters as mentioned in the related work section.

ACKNOWLEDGMENT

The publisher has waived the Open Access Processing fee for this article.
REFERENCES

Agarwal, A., Venkatadri, M., & Pasricha, A. (2018, December). Autonomic cloud resource management. In 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC) (pp. 138-143). IEEE.

Agarwal, A., Venkatadri, M., & Pasricha, A. (2019). Slab-based autonomic cloud resource management framework by ant lion optimization algorithm. International Journal of Innovative Technology and Exploring Engineering, 8(4), 119–123.

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. doi:10.1109/ICOIN48656.2020.9016522

Bosaeed, S., Katib, I., & Mehmood, R. (2020, April). A Fog-Augmented Machine Learning based SMS Spam Detection and Classification System. In 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC) (pp. 325-330). IEEE. doi:10.1109/FMEC49853.2020.9144833

Cherkasova, L. (1999). Scalable Web Hosting Service. HP Laboratories Technical Report HPL, (52/REV).

Dewangan, B. K., Agarwal, A., Choudhury, T., Pasricha, A., & Chandra Satapathy, S. (2020). Extensive review of cloud resource management techniques in industry 4.0: Issue and challenges. Software, Practice & Experience.

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.

Guerar, M., Merlo, A., Migliardi, M., & Palmieri, F. (2018). Invisible CAPTCHA: A usable mechanism to distinguish between malware and humans on the mobile IoT. Computers & Security, 78, 255-266.

Jain, A., & Choudhury, T. (2020). GAP: Hybrid task scheduling algorithm for cloud. Revue d’Intelligence Artificielle, 34(4), 479–485. doi:10.18280/ria.340413

Jones, M. D., Anderson, Z., Walker, C., & Seppi, K. (2018, April). PHUI-kit: Interface Layout and Fabrication on Curved 3D Printed Objects. In Proceedings of the 2018 CHI Conference on Computing Systems (pp. 1-11). doi:10.1145/3173574.3173684

Karande, V., Bauman, E., Lin, Z., & Khan, L. (2017, April). Sgx-log: Securing system logs with sgx. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (pp. 19-30). doi:10.1145/3052973.3053034

Koumidis, K., Kolios, P., Ellinas, G., & Panayiotou, C. G. (2019, December). Secure Event Logging Using a Blockchain of Heterogeneous Computing Resources. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE. doi:10.1109/GLOBECOM38437.2019.9013452

Layec, P., Dupas, A., Bisson, A., & Bigo, S. (2018). QoS-aware protection in flexgrid optical networks. Journal of Optical Communications and Networking, 10(1), A43–A50. doi:10.1364/JOCN.10.000A43

Lee, S., Choi, W., Jo, H. J., & Lee, D. H. (2019, July). How to securely record logs based on ARM trustzone. In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (pp. 664-666). doi:10.1145/3321705.3331001

Li, J., Tang, X., Wei, Z., Wang, Y., Chen, W., & Tan, Y. A. (2019). Identity-based multi-recipient public key encryption scheme and its application in IoT. Mobile Networks and Applications, 1–8.

Ma, M., Luo, M., Fan, S., & Feng, D. (2020). An Efficient Pairing-Free Certificateless Public Key Encryption for Cloud-Based IoT. Wireless Communications and Mobile Computing, 2020, 2020. doi:10.1155/2020/8850520

Ma, S. (2017). Authorized equi-join for multiple data contributors in the PKC-based setting. The Computer Journal, 60(12), 1822–1838. doi:10.1093/comjnl/bbx061

Ma, X., Yang, L. T., Xiang, Y., Zeng, W. K., Zou, D., & Jin, H. (2015). Fully reversible privacy region protection for cloud video surveillance. IEEE Transactions on Cloud Computing, 5(3), 510–522. doi:10.1109/TCC.2015.2469651
Mann, Z. Á., Kunz, F., Laufer, J., Bellendorf, J., Metzger, A., & Pohl, K. (2021). RADAR: Data Protection in Cloud-Based Computer Systems at Run Time. *IEEE Access: Practical Innovations, Open Solutions, 9*, 70816–70842. doi:10.1109/ACCESS.2021.3078059

Martin, J. (2021). Web Hosting Made Simple With These Easy Steps. *Techno Engineering Article, 1*(1).

Ogiela, L., & Ogiela, M. R. (2017, November). Security of visual codes in service management in the cloud. In *2017 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIIBMS)* (pp. 165-168). IEEE. doi:10.1109/ICIIIBMS.2017.8279717

Ouyang, Z., Zhai, X., Wu, J., Yang, J., Yue, D., Dou, C., & Zhang, T. (2021). A cloud endpoint coordinating CAPTCHA based on multi-view stacking ensemble. *Computers & Security, 103*, 102178. doi:10.1016/j.cose.2021.102178

Patil, S., Wasnik, K., & Bagade, S. (2019). Pen-Drive Based Password Management System for Online Accounts. In *Emerging Technologies in Data Mining and Information Security* (pp. 693–704). Springer. doi:10.1007/978-981-13-1951-8_62

Rane, S., Wagh, S., & Dixit, A. (2020, January). Design of a Forensic Enabled Secure Cloud Logging. In *Proceedings of the 21st Distributed Computing and Networking* (pp. 1-1). doi:10.1145/3369740.3373803

Ravi, N. C., Muppalaneni, N. B., Sridevi, R., Prasad, V. K., Govardhan, A., & Padma, J. (2018, December). Advanced Access Control Mechanism for Cloud Based E-wallet. In *International conference on Computer Networks, Big data and IoT* (pp. 392-399). Springer.

Song, H., Li, J., & Li, H. (2021). A Cloud Secure Storage Mechanism Based on Data Dispersion and Encryption. *IEEE Access: Practical Innovations, Open Solutions, 9*, 63745–63751. doi:10.1109/ACCESS.2021.3075340

Tian, H., Wang, J., Chang, C. C., & Quan, H. (2020). Public auditing of log integrity for shared cloud storage systems via blockchain. *Wireless Networks, 1–16*. doi:10.1007/s11276-020-02373-5

Valentine, T. (2021). Database-Driven Web Development Fundamentals. In *Database-Driven Web Development* (pp. 1-18). Apress. doi:10.1007/978-1-4842-5970-2_1

Vasco, M. I. G., Del Pozo, A. P., & Soriente, C. (2019). A key for John Doe: Modeling and designing Anonymous Password-Authenticated Key Exchange protocols. *IEEE Transactions on Dependable and Secure Computing.*

Vázquez, D. E., Hernández, E., & Meneses, A. (2018). Equivalence Relation Between Widgets for GUIs in Mobile Applications. *IEEE Latin America Transactions, 16*(7), 2007–2012. doi:10.1109/TLA.2018.8447369

Villasenor, S., Nguyen, T., Kola, A., Soderman, S., & Gu mànov, M. (2017, December). Scalable spam classifier for web tables. In *2017 IEEE International Conference on Big Data (Big Data)* (pp. 4849-4851). IEEE. doi:10.1109/BigData.2017.8258564

Vleju, M. B. (2014). Automatic Authentication to Cloud-Based Services. *Journal of Universal Computer Science, 20*(3), 385–405.

Xu, Z., Wu, L., Ren, Y., & He, D. (2018). New Efficient Certificateless Aggregate Signature Scheme. *Journal of Internet Technology, 19*(7), 2023–2033.

Yunakovsky, S. E., Kot, M., Pozhar, N., Nabokov, D., Kudinov, M., Guglya, A., & Fedorov, A. K. (2021). Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. *EPJ Quantum Technology, 8*(1), 14. doi:10.1140/epjqt/s40507-021-00104-z

Zeidler, C., & Asghar, M. R. (2018, August). AuthStore: Password-based authentication and encrypted data storage in untrusted environments. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 996-1001). IEEE.