Security and Privacy in the Cloud: A Balancing Act Between Innovation and Risk

Deepika Dhiman[1], Ms. Jaspreet kaur[2]

Department of Computer Application, Chandigarh School of Business, Chandigarh Group of Colleges, Jhanjeri, Mohali, India

deepikadhiman104@gmail.com[1] , jasPreet.j2249@gmail.com[2]

ABSTRACT

Though it offers unparalleled flexibility and scalability, the distributed nature of the computing raises a number of security and privacy concerns. This paper's goal is to clarify the many security and privacy concerns raised by cloud usage. We will study the current systems of protection, point out good existing technologies such as access control, encryption schemes, and trust mechanisms. Nevertheless, we recognize the persistent issues as well, such as multi-tenancy complexities, data sovereignty problems, and the continually changing threat environment. Eventually, we plan to offer further research directions to cover the gap between innovation and risk in order to build a more secure and privacy preserving cloud environment. The cloud provides a wealth of innovative ways to store and access data. This convenience has its own dilemma. Exposing the advantages of cloud-based technologies has to do with steering through the difficult territory of security risks and privacy violation incidences. This paper reviews the issue with an emphasis on the necessity of implementing strong security controls as well as data privacy issues. This paper calls for an active and holistic view on security and privacy issues in the cloud, one that recognizes the risk-innovation dilemma while striving for equilibrium. Organizations will have a framework to deal with the changing world of cloud computing as a result of the adoption and use of Cloud Guard. This way, there will be confidence, resilience, and integrity when innovating and protecting private and important information in the cloud. It exhorts the complexity facing in functioning the systems, analyzing the risks, and aligning to the incidents focusing on the security performer to remain proactive against any illegal intrusion and breach. Besides that, ethical issues of cloud security and privacy are considered that address data ownership, surveillance, and moral concerns which arise as the result of digital technologies.

KEYWORDS

Cloud security, Cloud privacy, Information security, Data protection, Access control, Encryption, Trust mechanisms, Multi-tenancy, Data sovereignty, Threat landscape, Cloud innovation, Security-privacy trade-off

I. INTRODUCTION

The word "cloud" in this context represents a big global network of these remote servers placed hundreds of miles away from each other, in data centres. Sometimes, those servers store information, execute programs and give online services collectively. Not only will you utilize your actual servers and hardware, but at the same time, you would be getting access to a huge pool of computing power whenever needed.

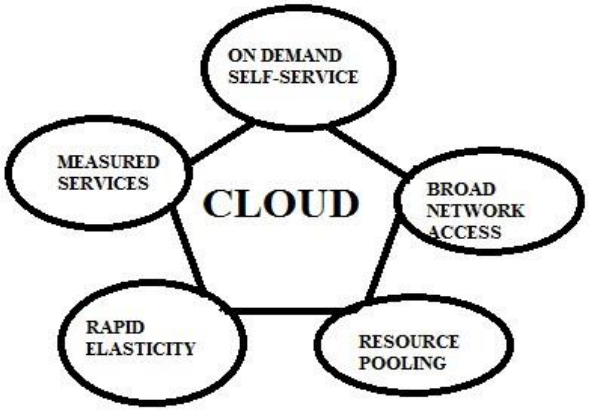

Figure1. Characteristics of Cloud

While in the non-stop debate of technological progress, the cloud has become a key challenge to change paradigm. Data, that used to be stored only on physical servers and kept in the premises, has now become a capable traveller over the virtual networks, being available for retrieval from any corner of the world with internet connection. This fresh freedom has brought a lot of volcanoes of creation. Then, the area of applications, shared workspaces, and the degree of independent adjustability have been put on a completely new level. The name Risicare that is the Italian verb and which means 'to dare' is the route to the English phrase "risk". The central idea of the word's creation is that risk is a decision which people make due to their different personalities or the situations around them by themselves as well as their ambience (Bernstein, 1998). This work unfolds the subtle web of cloud security and privacy; it further investigates the complex connections between risk management and innovation. Through amalgamating theoretical knowledge and empirical data as well as direct case studies the principal objective of this research is to clarify the broad spectrum of challenges and opportunities that are presented by the cloud environment. The realization that cloud computing via the Internet creates an opportunity for the arising of risk exposure and susceptibility despite the fact that it raised the scalability, flexibility, and costeffectiveness levels as never before is the grounds for the present research. The

rise in the number of cyber-attacking, data breaches and privacy invading make it imperative for the security of sensitive data in the cloud environment. Nevertheless, attaining the right balance requires taking into account a broad range of factors, including company culture, legality law, technology adaptation and ethics. Think about a globe where data is accessible from any place at any time overcoming the distance between two or more places. This is the sordid reality of cloud computing, a new system introduced into the world that revolutionizes the data storage and accessibility through science and technology. It creates a radius of creativity which rather is unnatural, stimulates confidence in young business people, and inspires coordination and team work. Nonetheless, there's talking point to this mini-world. Despite all the good things that could be attributed to cloud computing, it is also true that people were made aware of the risks of data security and the privacy of the information the cloud stores. This study explores this paradox: the cloud's capacity to promote advancement while also endangering the data that powers it. Among the remarkable things that happened to the digital world, the diffusion of the cloud is one of them. It lures you with a façade of a utopian idea to safeguard and process data. This digitized Eden is no free ride though. As we celebrate the cloud's infinite scalability and affordability, a sobering fact becomes apparent: safety and privacy problems are a matter of concern and may cause serious problems to central nature of cloud based applications which is trust. This research investigates the cloud's complex balancing process between risk and creativity to understand how the cloud works. We will analyse the absolutely evident benefits associated with cloud computing, such as fostering agility and collaborative environment as well as driving innovative research. On the other hand, we are going to put great emphasis on how cloud computing creates risks. A thorough analysis of the potential security loopholes and data border violations will hopefully allow us to pinpoint the complexity of the digital era. By the end of this post we are intending to lay the groundwork for a cloud that will always be creative and where the main pillars of its rapidly transforming digital world will be secure protocols and invariable user privacy.

The way the data is accessed and stored has undergone a deep transformation in the digital era. In the past, a cloud as a concept was considered a far-future idea, but in the present, the cloud is a ubiquitous force that delivers organizations and individuals with cost-effectiveness, scalability, and convenience in what we know now as an ideal answer. Yet, this technological miracle is so much like a double-edged one. Innovation is reaching new peaks with the cloud computing and at the same time the cloud service providers need to keep privacy and security intact as otherwise these leaks can cut the robust trust on which the whole cloud is positioned. We will evaluate the undeniable advantages of cloud computing only to compare it with the vulnerabilities and privacy issues that may arise when peoples' data is transferred to the virtual world. We aim to explore emerging paths by analyzing possible dangers, assessing the degree of cloud security at the present time, and thinking about new methods. By this path, creativity will be still instigated by the cloud, but effective security steps will ensure the protection and security of information (data) that drive this advancement. Here is the basic structure of the cloud computing, besides the principle and the effects of cloud computing on security and innovation. The grid is the pioneer of the cloud which is the latest advance in distributed architecture. The user is only required abstraction to encounter cloud infrastructure setup; no any special knowledge or background is required. It can be the carrier of high scalability, high throughput, and high quality service of the Internet with considerable processing power.

Cloud computing based common online business applications can be accessed via a web browser from the hosting servers by the providers. If there is the kind of situation where the cloud service is of inferior workmanship and the users feel this is not of the needed quality then they would not desire to make use for cloud services. Cloud suppliers cannot completely not to get rid of the risks at zero-level, although with good risk management strategy, they are safe and efficient since they control resources in the cloud and, therefore, buyers cloud will have technical insurance. Governmental information technology (IT) has gained a lot from cloud computing because it allows rapidly scalable applications as well as storage and platforms. Cloud computing providers offer a variety of services tailored to individual needs and institutional requirements as well as business operations. Cloud consumers apply cloud computing for information dissemination and storage of data, data base administration, mining of data and web service deployment. Along with the opportunities to process vast amounts of data and model the most complex scientific problems, computing in the clouds can also have implications for the management of health records (Hand, 2007). The agency utilization of cloud capabilities has developed more than in past years, after President Barack Obama's, and CTO Vivek Kundra's statements about their plan to check the cloud one of the leading parts of the federal IT transformation. As a megatrend that is commonly referred as the cloud computing, this is a fast-growing sector of the Internet Service Provider. Incorporating resource sharing, virtual memory supported by pay-as-you-go business model (PAYG) will let cloud service get its purpose which is cost reduction. In the sector of the cloud examples of services are the Google App Engine, S3, and the Amazon Elastic Cloud computing (EC2). Nevertheless, the threat of hacking cloud system providers between the security and privacy benefits of their apps and services is an essential factor.

II. EVOLUTION OF CLOUD COMPUTING

"Using computers as a public utility" the aero plane of cloud computing. Initially made in the 1950s. Listening: Instruction: Humanize the given sentence. There were 5 core things that gave birth to cloud technology as it we see it today. This includes virtualization, web 2.0, service orientation, distributed systems which are currently among the most modern technologies and utility computing which will become a trendy by 2010.

A. *Distributed systems:* Distributed systems are the result of few separate and individually existing independent systems constituting a single system for the user. In distributed systems, resources are allocated and shared (among others), using servers to make decisions and coordinating all actions in the system. Scales, concurrency at same way, continuous accessibility, along with variant component of distributed systems include error-resilience and heterogeneity. Therefore, there most likely was an issue with the deployment method since a

system was at each physical field. In addition to the mainframe, cluster, and grid being the three other forms of simplices that were derived from the distributed computing, they developed to solve the problem of limited computing power.

B. *Mainframe computing:* As the greatest word in computing engineering upheld for first time in 1951 by IBM, mainframes are still the very considerable and stable devices. These are responsible for the execution of complex computer-based processes that involve huge information input and output or other data-related activities. These are used for those jobs that involve vast processing, like virtual financial transactions, etc. Their system is fault in any case, just as one may say that the downtime is minimal. These two types of computing burnt into the air for multiple RAM tasks together to speed the CPU mulching up the data much faster. Nonetheless, they were very costly products. Cluster computing became a policy which replaced the mainframe technologies to combat the escalating prices.

C. *Cluster computing:* It was introduced as a paring of mainframe computing of late 80s. A high-bandwidth network let each node on this cluster connect to each other others. On the flipside, stations of this magnitude have used supercomputers that are costlier. Not overlooking the fact that such machine could accomplishes the most intricate calculations. Another significant benefit is that the addition of new nodes to the cluster is quite a straightforward affair. This, however, had a mixed effect; cost challenges were mostly dealt with, but the issue of geographic restrictions still stayed. Grid, which was the concept proposed as the way out of this problem, was responsible for the definition of the new paradigm, i.e. grid computing.

D. *Grid computing:* The concept of grid computing, which was firstly mentioned in the nineties, was much referred in later days. These set-ups suggest that a lot of places in varying geographical locations that had the web were actually connected. As these systems were interconnected and belonged to different organizations, the grid was highly dynamic and more nodes were included in it. It had certain major flaws in the program, like the communication over the distance between the nodes. So, more new issues came up. The biggest barrier that was identified in the process was low capacity backbone network communication, which also included a wide range of network-related issues. Therefore, on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service become the decisive features of cloud computing services. Consequently, cloud computing is often called "Grid Computing Successor".

E. *Virtualization:* Its dawn can be traced back to about forty years. It succinctly details the way in which a virtual layer is stacked on top of the physical machine to create a multimode environment where the user can concurrently run multiple instances of the hardware. Cloud computing will not be complete without this and is an essential part of the technology. It is upon this platform which a lot of existing cloud machines are built, among them being VMware vCloud, Amazon EC2, and others. It should be pointed out that even though software virtualization is the most widely used form of virtualization the hardware still occupies the number one place in this list.

F. *Web 2.0:* This refers to the frontend where clients and cloud computer interact. Our flashy, trendy, intuitive, and easily navigable web sites are all byproducts of Web 2.0. Not only is this feature has a hand in, but it also supports a site that can accommodate all screen sizes. The typical web 2.0 applications which are frequently used are Face book, Twitter, Google Maps and other tools which are in numerous. Already it represents no question that social media exists only because of this advancement. By the Year 2004, it earned good reputability.

G. *Service orientation:* The idea that a service orientation concept acts as a cloud computing reference paradigm. It helps in customizable, cost-feasible, and nimble solutions, thanks to its dynamism and flexibility. In this model, two principal notions that were explained are, namely. Those would cover SaaS (Software as a Service) and QoS (Quality of Service), which also at the same time implies the SLA (Service level Agreement).

H. *Utility computing:* The model of computing utility, basically, is how instead of having to buy all the components that you might need or use, you're able to pay per usage and get compensated with more services on top of the storage, infrastructure and computation services.

III. CLOUD SECURITY RISKS

A. *Data Breaches:* The larger cloud providers become, the more data they will have to store, hence if you are a malicious individual interested in stealing data, the cloud will be a very lucrative target. Breaches of data could be attributed to insiders who threaten information security, improper access control, and vulnerabilities in cloud computing systems.

B. *Shared Responsibility paradigm*: There is a busy shared responsibility strategy which is applied in many ways, and this is typically used in the context of cloud security. Whether it is the security of data or the accessibility of account a consumer is responsible for safely storing information and managing the permission to their account even if documentation is secured by the provider. As a consequence of configuration confusion and misconceptions of the shared responsibility, attack surface can grow.

C. *Emerging Threats:* cloud-based technologies including server less computing and containerization offer new attack vectors. As a result, there is a need of continual adaptation in security for the cyber world.

IV. THE SECURITY AND PRIVACY REGULATIONS WHICH SHOULD BE INCLUDED IN CLOUD

The security and privacy regulations should be included Security of data or information aims to protect their integrity, confidentiality, and availability. The access control (AAA), authorization, and authentication methods developed are also included. Privacy is the opposite of privacy and is governed by the law as well as society's non legal standards. Consent, purpose limitation and validity are its components which guarantee that the cloud computing deployment doesn't violate legal measures. Openness, Governance, and Compliance seem to make the list, too. Through the ISO it is also proposed that certain information security requirements be met in ISO 7498-2.

A. *Undefined identity and authentication management:* The obstacle of the multitenancy of the cloud which facilitates the usage of malevolent users or adversaries to use the system is the reason of the user identity and authentication difficulty in the cloud environment.

B. *Authorization and access control:* In a cloud system, particularly a public cloud, numerous users with varying privileges from around the globe can access the cloud. CSPs assign privileges to users according to the type of account they have. The difficulty here is in managing the cloud resource ownership, rights, and access priority of verified users. Keeping an eye on and managing the actions of those privileged users is also one of the trickiest issues.

C. *Non-repudiation:* facilitates an eradication of any chance that the sender or the receiver would have to eradicate existence of communication or the receipt. Treating with concepts like timestamps, digital signatures, and confirmation receipts services is the way to reach this goal.

D. *Integrity:* this thus makes certain that no aspect of the data has been tampered with including illegal SQL injection, DOS attacks, the theft of data and the addition of malware. Integrity goes with ACID as a protocol obviously and also touches data quality and completeness.

E. *Compliance and Audit:* To this end, the deployment of cloud must be in compliance with regulations and laws so as to allocate the general legislations and sector specific requirements. Thus, the privacy requirement involves making sure the cloud deployment is in compliance. CSPs have to strictly adhere to a set of standards which range from ISO/IEC 27001 to SAS 70 and from the Health Insurance Portability and Accountability Act to the Payment Card Industry Data Security Standard. A series of audits must be passed also. As cloud services are being widely popularized by users, it is crucial for those individuals to strictly bind by the software licenses while using different cord programs and with regard to cryptography rules while sending confidential information over public networks. Maintaining regulatory standards can often be a tough affair, since cloud service providers hardly know about what data is hosted in their infrastructure as well as its geographical location, which makes it hard to provide their clients a compliance report.

V. BALANCING INNOVATION AND RISK

The complex cloud security and privacy matters cannot be settled by employing one-solution-fits-all.

A. *Security Best Practices:* It is necessary to put powerful security mechanisms, such as access control, multifactor authentication and encryption in place. In proactive defense, threat identification and constant monitoring are the backbone of security operations.

B. *Regulation Compliance:* The demonstration of respect for user privacy is a result of compliance with applicable data privacy laws e.g. the CCPA and GDPR.

C. *User Empowerment and Education:* The trust and transparency in the cloud security can be promoted by explaining to users the connected dangers and the finetuning the data sharing processes.

D. *Cooperation among Stakeholders:* To foster solid security architectures and rightful data management policies, it is imperative that cloud service providers, government institutions and technology firms do together.

Figure2. Balancing Innovation and Risk in Cloud

VI. CLOUD SERVICE MODELS

Cloud services are typically associated with layers that reflect multiple service model types, each layer offering different functionality.

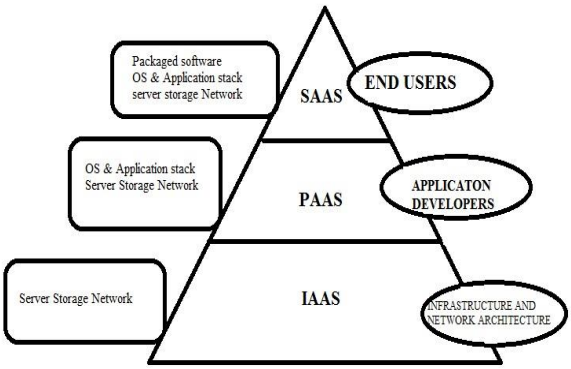

Figure3. Cloud Service Models

A. *IAAS (Infrastructure as a service):* In IaaS you pay to lease hardware or infrastructure hardware on demand. It is a pool of networked resources located on the Internet. By using IaaS benefits users to reduce the cost for and the technicality of buying and maintaining the physical servers. Examples are: DigitalOcean, Linode, Amazon Web Services (AWS), and Azure from Microsoft.

B. *PAAS (Platform as a service):* With the PaaS cloud computing platform developers can create, test, spin up, and run web apps. Examples are: Azure Windows, Heroku, Google App Engine, and OpenShift.

C. *SAAS (Software as a service):* SaaS is technological cloud-based service also referred to as "the software on demand". It is software in which the company hosting the applications is being using the cloud service provider as a back-end. People can use these applications with a web browser and (the) internet connection. Examples are: Ex.: BigCommerce, Google Apps, Dropbox, and Slack.

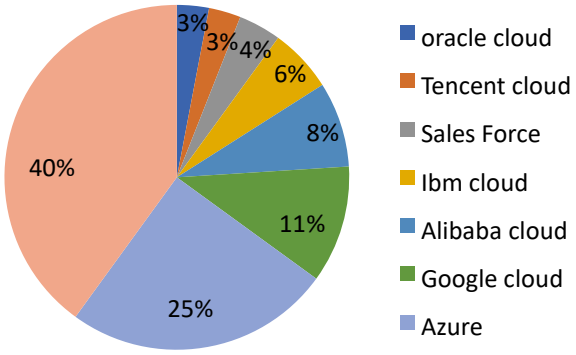

Figure4. Largest cloud Companies

VII. CLOUD DEPLOYMENT MODELS

Cloud Deployment models are categorized in four parts as follows:

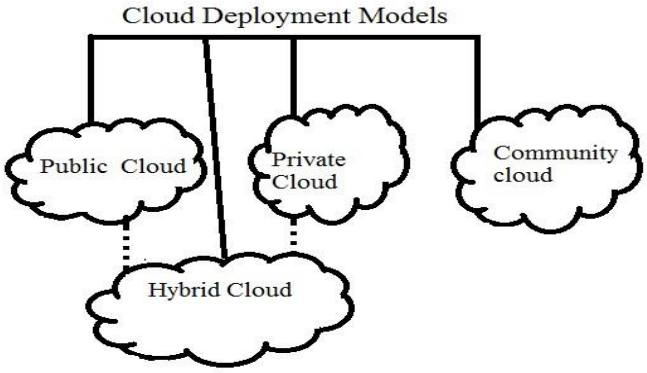

Figure5. Cloud Deployment Models

A. *Public Cloud:* This information is available to all. Public cloud platforms fit well for organizations that has variable, but disparately growing, demands. It also fits in well with low-security specification.

B. *Private cloud:* The private cloud gives more headway that allows the user satisfaction as per the organization demands when it is necessary to have it personalized. It is also an intelligent approach for the ones that are on a continuous development track or have incorporate fast changing requirements.

C. *Community cloud:* Public cloud market works in more or less identical way to the community cloud. It is different one – the access is given only to a subset of the people which have common objectives and they are trying to solve same problems. This model of cloud computing deployment is internally managed and hosted or may be hosted by the vendor.

D. *Hybrid cloud:* A hybrid cloud itself involves two or more types cloud architectures. Each model at the heart of hybrid cloud is independent while all of them are integral part of architecture.

VIII. THE CHALLENGES INCLUDE IN CLOUD

A. *Balancing Act:* It can be very challenging to maintain that balance between security objectives and environmental aims.

B. *Evolution of Threat Landscape:* Without a doubt, the hackers will be constantly updating their practices in parallel with the development of sustainable cloud infrastructures, thus creating additional problems.

C. *Lack of visibility:* many companies do not recognize the exact points where they process and keep their data though their apps, or where they the inventory assets are kept.

D. *Reduced authority:* For them, the way data is handled using apps are at the mercy of third-party infrastructure platforms' rules and regulations.

E. *Doubt about shared accountability:* A shared cloud security responsibility model involving business and cloud service providers may lead to breaches or inappropriate access if roles and responsibilities are blurred or poorly demarcated.

F. *Uneven reporting:* But, increasingly many companies are finding out than the multicloud, and the hybrid cloud solutions are more suitable to their objectives, however, the varying of the service suppliers is offering a different level of functionality and geographic coverage, which may result in uneven security.

IX. PROSPECTS OF CLOUD

A. *Innovation Spur:* It is possible for new cloud architectures, algorithms and protocols to appear if the couple goals of sustainability and security are achieved.

B. *Stakeholder Engagement:* Handling with sustainability may also be a source of more interactive relationships with stakeholders like customers and regulators, thereby,

promoting the function of the team in the struggle of security.

X. THE FUTURE OF CLOUD COMPUTING 2025-2030

The continued rise of hybrid and multi-cloud methods: We expect that the deployment of these approaches will continue with the constantly growing popularity of organisms using more than one cloud provider. This gets the businesses to use each provider's key strengths and unique offerings without trying to do it all by themselves.

A. *The continued rise of hybrid and multi-cloud:* One of the main drivers for edge computing will be the rising need of computing capability at the networks edge which will occur along the development of the Internet of Things. Consequently, edge computing architectures, as opposed to centralized cloud models that may often result in higher latency and poorer performance, will become widely used.

B. *Increased AI and machine learning:* The cloud market players will spare not penny in science of AI and cyber security. Thanks to this, they will enable a more developed features and services to be provided, including, say, intelligent systems and automatic scalability.

C. *Increased emphasis on security:* With the growing of cloud computing there will be a corresponding increase on security. Tightened up regulations regarding data security, access, and usage and increased investment funds into technologies aimed at data security are forthcoming.

D. *Continued price wars:* Given the fact that there are overwhelming numbers of actors battling for a place in the sun, the industry is going to continue the trend of price war. They can profit from it as long as its introduction is followed by a product price drop.

E. *More regulation:* Cloud services are multiplying and we should expect more laws that would ensure security, privacy, and other issues. Consequently, such regulation option will be able to provide users' rights with protection and accountability for the doers of providers.

XI. CONCLUSION

In a wrap, the cloud computing has indeed completely transformed how data is on demand by all gaining greater impetus and flexibility never heard before. In addition to many benefits these solutions bring, we should take into consideration the list of risks, most importantly related to the security and privacy. Cloud direction has been from mainframe to the present hybrid and multi-cloud type which hosts a number of prototype ideas as well problems. An issue we always know is how we will balance innovation while striving to mitigate risks. It thus requires that there are necessary protection measures that ensure regulatory compliance, user education, and stakeholder participation among others. The way cloud computing will be like in the future can be predicted with some confidence; a set of trending patterns can be listed in this regard that comprise of the persistence of the hybrid-cloud and multi-cloud architecture, rise of the security-consciousness, influence of AI and machine learning, price competition, and more strict regulations.

REFERENCES

[1] Boopathi, S. (2024). Balancing Innovation and Security in the Cloud: Navigating the Risks and Rewards of the Digital Age. In Improving Security, Privacy, and Trust in Cloud *Computing* (pp. 164-193). IGI Global.

[2] Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, 1-22.

[3] Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in iot-based cloud computing: A comprehensive survey. Electronics, 11(1), 16.

[4] Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government information quarterly*, *27*(3), 245-253.

[5] Abioye, T. E., Arogundade, O. T., Misra, S., Adesemowo, K., & Damaševičius, R. (2021). Cloud-based business process security risk management: a systematic review, taxonomy, and future directions. *Computers*, *10*(12), 160.

[6] Pearson, S. (2013). Privacy, security and trust in cloud computing (pp. 3-42). Springer London.

[7] Abdulsalam, Y. S., & Hedabou, M. (2021). Security and privacy in cloud computing: technical review. Future Internet, 14(1), 11.

[8] Ali, A., Warren, D., & Mathiassen, L. (2017). Cloud-based business services innovation: A risk management model. International Journal of Information Management, 37(6), 639-
649.

[9] Martens, B., & Teuteberg, F. (2012). Decision-making in cloud computing environments: A cost and risk based approach. Information Systems Frontiers, 14, 871-893.

[10] Barona, R., & Anita, E. M. (2017, April). A survey on data breach challenges in cloud computing security: Issues and threats. In 2017 International conference on circuit, power and computing technologies (ICCPCT) (pp. 1-8). IEEE.

[11] Youssef, A. E., & Alageel, M. (2012). A framework for secure cloud computing. International Journal of Computer Science Issues (IJCSI), 9(4), 487.

[12] Kalloniatis, C., Mouratidis, H., Vassilis, M., Islam, S., Gritzalis, S., & Kavakli, E. (2014). Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. Computer Standards & Interfaces, 36(4),
759-775.

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

[14] Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. International Journal of Information Management, 43, 146-158.

[15] Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers, 1-22.

[16] Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.

[17] Habbal, F. (2018). Big data: balancing between risks and opportunities–UAE perspective. International Journal of Economics and Business Research, 15(4), 453-462.

[18] Brender, N., & Markov, I. (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. International journal of information management, 33(5), 726-733.

[19] Maple, C. (2017). Security and privacy in the internet of things. Journal of cyber policy, 2(2), 155-184.

[20] Kuyoro, S. O., Ibikunle, F., & Awodele, O. (2011). Cloud computing security issues and challenges. International Journal of Computer Networks (IJCN), 3(5), 247-255.