International Journal of Engineering, Science and Mathematics
Vol.8Issue 9, September2019,
ISSN: 2320-0294 Impact Factor: 7.875
Journal Homepage: http://www.ijmra.us, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

CLOUD COMPUTING FOR GOVERNMENT ORGANIZATION IN INDIA - AN EXPLORATORY APPROACH

Ashwini Parab[1], Dr. Vijay Pal Singh[2]
Department of Computer Science & IT
[1,2]OPJS University, Churu, Rajasthan.

ABSTRACT:

In today's digital world, the Internet is revolutionising the way we work, learn, and interact. E-Government and business may be effectively linked through the cloud since it allows for the sharing of resources such as infrastructures, software, and applications between departments. A number of governments are struggling to keep track of unresolved papers that have been brought to the attention of the authorities as well as document verification for a variety of statements that they have been unable to address over the course of the year. Using cloud-based e-governance to solve these problems and improve e-governance services is essential. Using cloud e-governance software, citizens can easily access government services and carry out transparent actions. This article investigates India's experience with cloud computing and cloud-based e-governance, as well as the challenges of doing so in e-government applications.

Keywords: Cloud Computing Services, India, ITC, E- Governance and Cloud based E-Governance.

1. INTRODUCTION:

A revolution in communication, education, and employment is underway, thanks in large part to the remarkable success of the Internet and its rapid expansion **(Smitha, K.et al, 2012).** Since traditional distributed computing infrastructure is not as flexible, trustworthy, or high-performing as cloud computing, it's been one of the most significant developments in the IT sector in recent years **(Dash, S., & Pani, S. K, 2016).** We can also observe that governments are taking proactive initiatives to plan new ways of interacting, improve services, streamline processes, and revitalise democracy through increasing IT spending.... It aims to improve the quality of life for citizens and businesses by implementing e-governance **(Varshney, R. 2019).** New developments in cloud computing are making it easier for developing countries to establish E-governance services while also improving the quality of service they can offer their citizens**(Rastogi. A, 2010)**

2. LITERATURE REVIEW:

"The cloud is a virtualization of resources," **A Singh (2019)** explains. "It gives users with on-demand access to virtualized resources." Additionally, cloud computing's numerous advantages touch the government sector. As a part of this research, I explore how cloud computing is becoming more popular in the government sector around the world. **K. Mukherjee and S. Maurya (2018).** On-demand access is provided via the cloud's virtualization of resources such as network infrastructure (e.g., apps, servers, services, and data storage). The many advantages of cloud computing also have an impact on the public sector. **A. Johar et al (2019)** Scalability, availability, and reliability are just some of the advantages that cloud computing offers. Despite the fact that big data solves many of today's problems, it still contains substantial weaknesses, or gaps, that create concern and require rectification. Security, disaster recovery, scalability and privacy are only few of the difficulties that remain unanswered in the field of data management. All three of **J. L. Zittrain's books (2019)** There has been a dramatic shift in public thinking about digital governance since the late 1990s, and this shift must be taken into account in order to comprehend where it's going. In **A. Clarke (2017)** In the face of today's governments' overpriced and underperforming digital services, as well as lagging digital transformation goals, Digital Government Units (DGUs) have quickly emerged as a preferred alternative. When it comes to DGUs, they share a common set of values and practises that include agile, user-centered design and open source technology, pluralistic procurement of goods or services, data driven decision-making, horizontal "platform" solutions, and an emphasis on "delivery-first" mentality.

i) CHALLENGES FOR THE ADOPTION OF CLOUD COMPUTING IN INDIA:

Two India's big problems with cloud adoption include a lack of data security and internet availability in rural areas. Because data saved in the cloud needs to be protected to the same degree as data stored locally, government agencies are focused first and foremost on maintaining tight control over their data. The secrecy and security of government data is also a concern, as it is stored on a public network and so vulnerable to interception.

Because the user's location may be geographically far from the cloud, as well as according to how fast the internet is and how many people are using the data simultaneously, there is a second problem with cloud computing. Consumers are also concerned about vendor lock-in, service provider reliability, pricing fluctuation over time, and other issues. In no way can a vendor promise that the platform will always be operational.

ii) CLOUD-BASED E-GOVERNANCE IN INDIA:

Governments around the world are adopting new methods of participation in the governance process, and India is leading the way in this shift. India's government is currently in the process of integrating ICT into its operations **(Kumar, P. et al. 2020).** All of India's state governments are using some form of e-Governance system. E-governance is becoming increasingly dependent on cloud computing. Cloud computing technologies can be used to provide cost-effective e-Government solutions. They can be distributed throughout a wide area, resulting in better service quality for the end customer. Access to government services is made possible through the G-cloud (Government on Cloud). E-governance models must be put in place, but they must also be promoted to the general public **(S. Shibu and A. Naik, 2017).**

In cloud computing, SaaS, PaaS, and IaaS are the three service models that can be used to provide software, platform, and infrastructure (IaaS). It is up to the cloud provider to choose which service model is most appropriate for a given government requirement. Services It is necessary that cloud computing services be able to interoperate with one other and to be scalable, elastic, and portable. Cloud services can help the government take advantage of these advantages. It is critical that the government's use of resources be flexible, such that the amount of resources the government uses varies from time to time, with the government sometimes needing more resources and other times have resources that are free and unnecessary. Cloud computing's elasticity allows the government to save money by increasing or decreasing the quantity of resources accessible.

Network Infrastructure Readiness: - When a large number of citizens visit government websites at the same time, the network infrastructure is able to accommodate the increased bandwidth demand. When government websites are moved to the cloud, a thorough examination and audit of all network infrastructure areas is required.

Government Readiness: - Consider whether the government is ready to move to the cloud before making any decisions. The government has to decide which services can be moved to the cloud. The government and the cloud service provider must sign a Service Level Agreement (SLA) that includes all service terms and conditions, as well as security.

To ensure that the government's data is safe when it moves to the cloud, security is the primary consideration. It's important to know whether or not a cloud service provider can provide the same or superior security as a government agency. The following security problems must be addressed when moving government data to the cloud.

• Statutory Compliance - Make sure to follow all applicable laws, rules, and regulations..

• Data characteristics - Evaluation of the basic security needs for the application data set..

• Confidentiality and privacy — preventing unauthorised access to data and information, whether by intent or by accident.

• The data should be accepted, comprehensive and correct.

• Governance – Ensuring that the cloud service provider's transparency, security and management are maintained. • Data control and access policies – Identifying where the data is stored and who has access to it. Along with the cloud vendor making sure they supply their clients with accurate information. Cloud service providers need tools and procedures that let them to specify and generate pricing schemes, as well as protocols that support service publication trading and accounting..

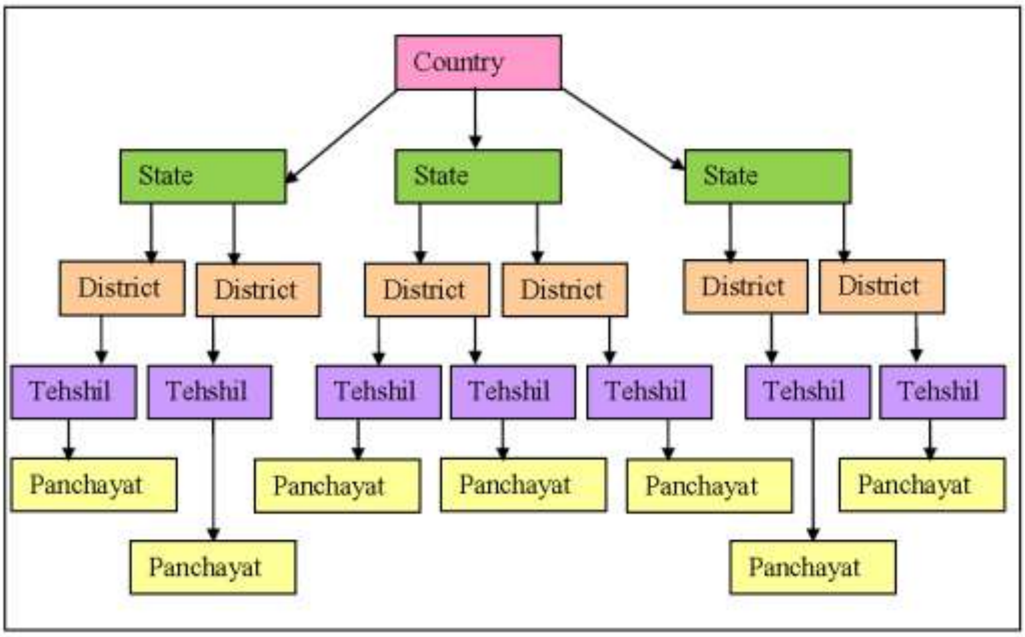

Figure 1: E-governance Model in India

3. METHODOLOGY:

To ease communication between the service provider (the government) and the user, the government's information system recommends the usage of identity federation and authentication (public). Additionally, the threat of unauthorised access to critical data comes not only from invaders but from hostile government workers. Protecting government information systems' valuable data and information is a top priority for the government. When it comes to protecting data and information systems, verifying the identity of its users is an important step. The process of verifying a person's identity before enabling them to access a system is known as user identification and authentication.

Using the computer's built-in hardware (hard disc and CPU) to authenticate a device is a useful method for government information systems, according to this study. In order to produce a string, we extract the hard drive's serial number and the total hard disc space using Windows APIs. These strings are then encrypted using a key to generate an authentication string. It will be stored on the authentication server, together with the user name and password. The identical string created from the user's computer using the same technique is compared to the string saved in the authentication server after authentication. By using this method you may ensure that both you and your machine are authenticated. Since most government computers are already fixed, this process is easy to implement. You don't have to buy a separate gadget for this way to work. Hardware device authentication with login and password for government systems and security was examined in this research..

Hardware equipment like a CPU, hard drive, or USB device can be used for authentication. Serial numbers are inscribed on the body of each piece of hardware by the manufacturer and can be used to authenticate the device. Changing the serial number of these gadgets is not an easy task.

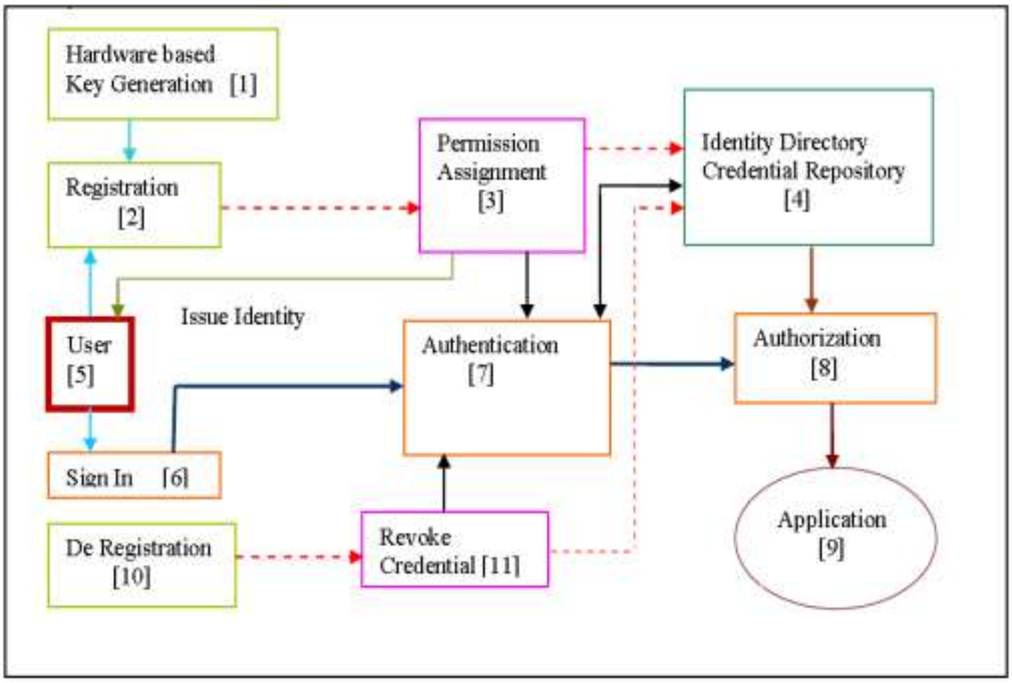

Figure 2: Device Authentication Process Diagrams

For increased authentication security, most government agencies have fixed computers that can be used for device authentication. An authentication key based on the hard disc serial number and total hard disc capacity is what this research is aiming to achieve. As part of the signup process, a unique key will be generated, which will be stored in the authentication table alongside the user's password. The government's web portal will prompt users to provide their login and password while trying to visit a government server. A key is generated from the user's computer using the same algorithm used to produce the key during registration if the user's login and password match those recorded in the authentication table. The user will be permitted access to the government web site's data and information if the generated authentication key matches the authentication key in the authentication table. A block diagram of the full authentication process is shown in the figure below..

4. RESULT:

The authentication server is responsible for verifying a user's identity when they attempt to access government information or data. In order to get into the government portal, the user will enter their username and password on a client PC and try to log in. The government's authentication server will check to see if the username and password are valid. The server will display an invalid message if the user is invalid. When a new user is formed, the client computer generates an authentication key if the person is legitimate. Client computers are authenticated by the authentication server by comparing a generated key with a stored key as well as the user name and password. The server will return an invalid computer error if the key is incorrect. If the key is the same, the server will allow the user to connect to the data server and send valid user messages if the key matches. It is now possible for a data server user to retrieve the information he or she needs after receiving validation from the authentication server. Examples of this process's applications include government portals and web-based applications. Information for the general public as well as critical data for the government can be found on these portals. Same and different strings (keys) are shown in the graph below.

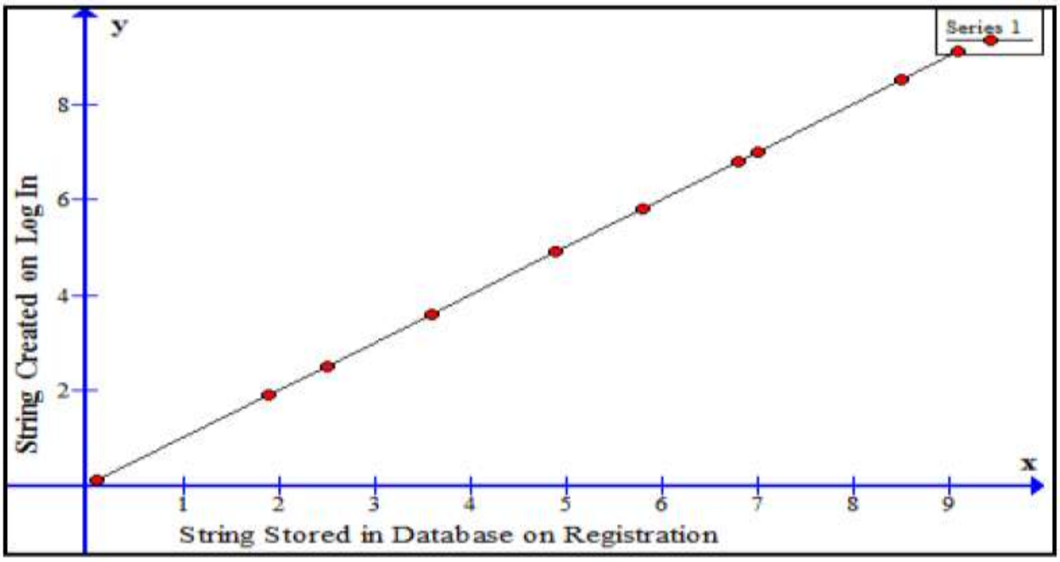

Figure 3:Graph: Same Strings

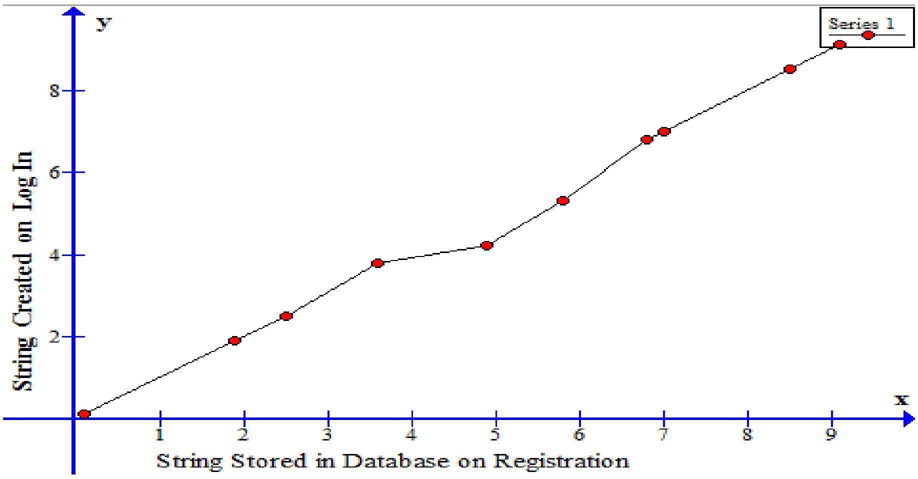

Figure 4: Graph: Different Strings

5. CONCLUSION:

An information security model for government information systems and security was developed after an extensive investigation and analysis of the subject matter. The government's web portal will prompt users to provide their login and password while trying to visit a government server. A key is generated from the user's computer using the same algorithm used to produce the key during registration if the user's login and password match those recorded in the authentication table. The user will be permitted access to the government web site's data and information if the generated authentication key matches the authentication key in the authentication table. Device-based authentication provides an alternative and better security in the domain following a thorough analysis of both technical and adoption aspects of device-based authentication across hybrid cloud architectures.

REFERENCES:

1. Smitha, K. K., Thomas, T., & Chitharanjan, K. (2012). Cloud based e-governance system: A survey. *Procedia Engineering*, *38*, 3816-3823.
2. Dash, S., & Pani, S. K. (2016). E-Governance paradigm using cloud infrastructure: benefits and challenges. *Procedia Computer Science*, *85*, 843-855.
3. Varshney, S., Sandhu, R., & Gupta, P. K. (2019, April). QoS based resource provisioning in cloud computing environment: a technical survey. In *International conference on advances in computing and data sciences* (pp. 711-723). Springer, Singapore.
4. Rastogi, S., Bhushan, K., & B Gupta, B. (2015). A framework to detect repackaged android applications in smartphone devices. *International Journal of Sensors Wireless Communications and Control*, *5*(1), 47-57.
5. Kaur, A., Gupta, P., Singh, M., & Nayyar, A. (2019). Data placement in era of cloud computing: a survey, taxonomy and open research issues. *Scalable Computing: Practice and Experience*, *20*(2), 377-398.
6. Maurya, S., & Mukherjee, K. (2018). An energy efficient design of cloud of things (CoT). *Journal of Information and Optimization Sciences*, *39*(1), 319-326.
7. Dong, S., Johar, M. S., & Kumar, R. L. (2019). Design of contracts and workflows for knowledge intensive IT service environments. *Decision Sciences*, *50*(3), 418-458.
8. Vijai, C. (2020). Cloud-Based E-Governance in India. *International Journal of Management*.
9. Zhao, L., Zhang, M., Shen, H., Zhang, Y., & Shen, J. (2017). Privacy-preserving outsourcing schemes of modular exponentiations using single untrusted cloud server. *KSII Transactions on Internet and Information Systems (TIIS)*, *11*(2), 826-845.

10. Jegadeesan, S., Azees, M., Kumar, P. M., Manogaran, G., Chilamkurti, N., Varatharajan, R., & Hsu, C. H. (2019). An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications. *Sustainable Cities and Society*, *49*, 101522.

11. Shibu, S., & Naik, A. (2017, August). An approach to increase the awareness of e-governance initiatives based on cloud computing. In *2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC)* (pp. 1-4). IEEE.