Initial Project Proposal: Group 2-1

Project Title:

Provisioning and De-provisioning for Identity Management in Cloud Computing from Service Provider's Perspective Using Blockchain and Machine Learning

Group Members:

Name	Email Id
Akash Roshan Mund (Leader)	armund@asu.edu
Bhavani Priya Kuche (Deputy Leader)	bkuche@asu.edu
Amey Bhilegaonka	abhilega@asu.edu
Kasi Kishore Ravuri	kravuri@asu.edu
Mahita Singamsetty	msingams@asu.edu
Naveen Aaditya Chitirala	nchitira@asu.edu
Rohit Vishwanath Badugu	rbadugu@asu.edu

Objective:

Identifying the security issues in the domain of provisioning/de-provisioning user access in identity management on cloud computing and automating the process using ML, Blockchain and illustrate how tools can be built to monitor continuously by adding a extra layer of security.

Motivation:

The purpose of this study is to illustrate the important aspects of provisioning and de-provisioning of Identity Management. When a new employee is hired, a record gets created in the organization database. The employee receives access to all of the required apps, accounts, and systems. During offboarding de-provisioning is needed to

safeguard confidential information. Other issues in provisioning and de-provisioning which are virtualization and phishing attacks are not considered as important as the advantages[8]. Furthermore, by using machine learning and blockchain, the above mentioned issues are handled which we will be exploring in our project.

Scope of Study:

In this project, from the service provider perspective, we will focus on security issues related to Identity management in provisioning and de-provisioning for Identity Management from the service providers view. Networks that weren't built for external access are suddenly being accessed regularly by BYOD devices and from locations the corporate has no control over. Using techniques such as blockchain and machine learning we will secure role-based access control to enable provisioning, and improve functionalities like scalability, integrity, and reliability by automating the process.

Expected Major Results:

- Recognize the major issues in securing cloud from service providers perspective
- Determining the steps to be followed inorder to secure the cloud resources which account for provisioning and de-provisioning for Identity management
- Determining the measures for preventing data breaches for security in cloud computing
- Understanding the technological link between Machine Learning and Blockchain
- Training the machine learning models to detect and mitigate the threats
- Understanding the Blockchain technology to ensure data security inorder to maintain liability of Identity management

Responsibilities:

Member Name	Responsibilities

Akash Roshan Mund	• Assigning weekly milestones for the smooth progress of the project • Discussing with team members to know their interests and distributing tasks accordingly. • Holding weekly meetings to get status on a weekly milestone • Discussing with Professor and TA to keep the project on track. • Reviewing and editing the weekly report to deliver error-free weekly reports. • Analysing research paper and security issues related to Identity management in cloud computing.
Bhavani Priya Kuche	• Interacting with group members to get a status update and taking leader's responsibilities in absence. • Keeping track of weekly report submission • Deep analysis of probable solutions to security issues related to identity management in cloud computing • Literature review on handling security issues using blockchain • Compiling analysis done by team members to come to a common ground

Amey Bhilegaonkar	• Review papers related to Security issues that can be resolved using blockchain and machine learning. • Detailed study on how blockchain and machine learning can improve identity management in cloud computing. • Compiling analysis data related to blockchain and machine learning to find suggestions on preventing security attacks.
Kasi Kishore Ravuri	• Finding resources on the project topic • Keeping track with the latest inventions and techniques using blockchain and machine learning that can help on improving identity management • Finding the best possible course of action given two technology for the same situation
Mahita Singamsetty	• Analysing existing solution to the problem in hand and how that can be improved. • Finding out unexplored techniques to resolve the problems. • Literature review on how to make the system more fault tolerant, immutable, and decentralized using blockchain. • Reviewing cloud computing system architecture to comprehend chances for security threats.
Naveen Aaditya Chitirala	• Study of elementary machine learning techniques that can be used to improve identity management in cloud computing. • Gathering information focused on machine learning that can bring solutions to problems

	• Analysing machine learning models that are best for the security of data.

Rohit Vishwanath Badugu	• Reviewing publications closely related to security issues related to identity management in cloud computing. • Accessing probable security threats and finding efficient ways to prevent the threats • Integrating blockchain approach with machine learning to find the best possible resolution for the problem
Everyone	• Building final project report • Engaging with the team and staying updated on project progress • Contribution towards weekly report

References:

[1] Stephen S. Yau, Ho G. An (2010). Confidentiality Protection in Cloud Computing Systems, Vol.4, No.4, pp. 351–365. http://ijsi.cnjournals.com/ch/reader/create_pdf.aspx?file_no=i68&flag=1&journal_id=ijsi&year_id=2010

[2] S. P. Otta and S. Panda, "Decentralized Identity and Access Management of Cloud for Security as a Service," 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS), 2022, pp. 299-303, doi: 10.1109/COMSNETS53615.2022.9668529.

[3] Shu Yun Lim,Pascal Tankam Fotsing,Abdullah Almasri,Omar Musa,Miss Laiha Mat Kiah,Tan Fong Ang and Reza Ismail,"Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey," International Journal on Advanced Science, Engineering and Information Technology, vol. 8, no. 4-2, pp. 1735-1745, 2018. http://dx.doi.org/10.18517/ijaseit.8.4-2.6838.

[4] Tomas Mikula, Rune Hylsberg Jacobsen (2018). Identity and Access Management with Blockchain in Electronic Healthcare Records, https://ieeexplore.ieee.org/document/8491888

[5] Bouras, M.A.; Lu, Q.; Zhang, F.; Wan, Y.; Zhang, T.; Ning, H. Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. Sensors 2020, 20, 483. https://doi.org/10.3390/s20020483

[6] Butt, U. A., Mehmood, M., Shah, S. B., Amin, R., Shaukat, M. W., Raza, S. M., Suh, D. Y., & Piran, M. J. (2020). A review of machine learning algorithms for cloud computing security. Electronics, 9(9), 1379. https://doi.org/10.3390/electronics9091379

[7] Qayyum, A., Ijaz, A., Usama, M., Iqbal, W., Qadir, J., Elkhatib, Y., & Al-Fuqaha, A. (2020). Securing Machine Learning in the cloud: A systematic review of Cloud Machine Learning Security. Frontiers in Big Data, 3. https://doi.org/10.3389/fdata.2020.587139

[8] Ashish Singh, Kakali Chatterjee. “Identity Management in Cloud computing Through Claim-Based Solution” 2015 Fifth International Conference on Advanced Computing & Communication Technologies, 2015, Vol.2015-, p.524-529

https://ieeexplore-ieee-org.ezproxy1.lib.asu.edu/stamp/stamp.jsp?tp=&arnumber=7079139