SECURE MODERN WORKSPACE'S POLICY MANAGEMENT USING AZURE AI

Ms. J. Akshaya[1], Ms. M. Nirosha[2], Ms. M. Nivedha[3], Dr. S. Venkatalakshmi[4]

[1-3]Student, IV Year, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai.
[4]Associate Professor, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai.

---***---

ABSTRACT:

To create a Modern workspace-based policy management with multiple level authoring and approval with both publishing and consumption views. Companies have their policies created and maintained locally within their legal department and/or by individual policy owners. These documents reside in the local computers of the policy owners and sometimes in multiple locations, without suitable controls. In order to overcome this business problem, we are going to create an entitlement-based platform where users can create their own policies, have them approved through a workflow based on metadata information within SharePoint and then view them and edit in future revisions. This system will also feature an AI based records management function to take care of regulatory functions based on certain business criterion. The above will be achieved using existing public cloud based cognitive services. This will also leverage microsoft office 365 graph API that allow use of the microsoft office software suite over the life of the subscription, as well as cloud based software as a service products for business environments.

Keywords: Policy, AzureAI, Cloud Services, sharepoint, Microsoft Office 365.

INTRODUCTION

All Organizations have created their policies and maintained locally within their legal department and /or by individual policy owners or HR team. Keeping data up-to-date in a database system is critical inorder to maximize the value of an organization's data assets[1]. In order to overcome this business problem, we are going to create an centralized platform using SharePoint where users can create their own policies and have them approved through a workflow based on metadata information within SharePoint and can view them and edit in future revisions. The framework enables the automated verification of properties regarding both the authorizations enforced by single policies and the relationships among multiple policies[3].Power automate is used to help in multiple level authoring workflow. Retention and compliance center are being used to help in the retention of the documents for a certain period of time. Azure protection service helps in protection of documents from unauthorized access. And azure AI is used for PDF conversion of the policy documents where all the employees of the organization can access them through a common platform and Microsoft office 365 platform is used for security purposes .A classification of the anomalies that can appear when designing or implementing communication protection policies[6]. In this all the policies are approved through a hierarchy of approvals starting from policy owners and then being approved by HR members, Legal members and finally approved by Board members. microsoft's cloud-based identity and access management service, which helps your employees sign in and access resources. Policy management needs to be flexible in order to adapt to different environments and be able to support policy evolution[9]. This will also leverage Microsoft office 365 graph API that allow use of the microsoft office software suite over the life of the subscription, as well as software as a service products for business environments cloud-based software as a service products for business environments.

ARCHITECTURE

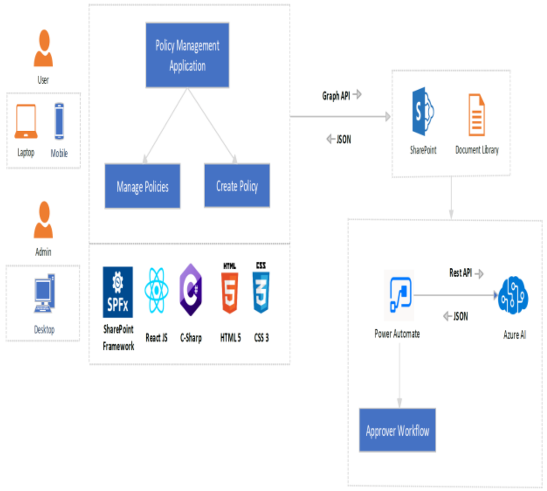

Fig: Modern workspace-based policy management

Architecture diagram defines the detailed solution recommendation for developing the policy management application in Office 365 Platform. It to support provable policy decision making and verifiable attribute tokens among multiple authorities[7].

- **Office 365 -** Primary application platform.

- **SharePoint Online** – Repository for storing the policy documents.
- **SPFx** – for developing custom form and grid web parts.
- **Power Automate** – For approval & email notifications workflow.

The model used is pre-trained with an extensive corpus of text and sentiment associations. It utilises a combination of techniques for analysis, including text processing, part-of-speech analysis and word associations[8].

RELATED SEARCH

1. Wei Zong, Freng Wu, Zhengrui Jiang proposed that in order to maximize the value of an organization's data assets, it is important to keep data in its databases up-to-date. In the era of big data, however, constantly changing data sources make it a challenging task to assure data timeliness in enterprise systems. For instance, due to the high frequency of purchase transactions, purchase data stored in an enterprise resource planning system can easily become outdated, affecting the accuracy of inventory data and the quality of inventory replenishment decisions. Despite the importance of data timeliness, updating a database as soon as new data arrives is typically not optimal because of high update cost. Therefore, a critical problem in this context is to determine the optimal update policy for database systems. In this study, we develop a Markov decision process model, solved via dynamic programming, to derive the optimal update policy that minimizes the sum of data staleness cost and update cost. Based on real-world enterprise data, we conduct experiments to evaluate the performance of the proposed update policy in relation to benchmark policies analysed in the prior literature. The experimental results show that the proposed update policy outperforms fixed interval update policies and can lead to significant cost savings. Keeping data up-to-date in a database system is critical in order to maximize the value of an organization's data assets. However, constantly changing data sources often make it a challenging task to assure data timeliness in enterprise database systems. Because enterprise resource planning (ERP) systems are one of the most widely adopted types of software systems in today's organizations. We use ERP systems to illustrate the challenges, the solutions, and the benefits of achieving data timeliness in a modern database system.

2. Puneet Gupta, Scott D. Stoller and Zhongyuan Xu has demonstrated that in large organizations, access control policies are managed by multiple users (administrators). An administrative policy specifies how each user in an enterprise may change the policy. Fully understanding the consequences of an administrative policy in an enterprise system can be difficult, because of the scale and complexity of the access control policy and the administrative policy, and because sequences of changes by different users may interact in unexpected ways. Administrative policy analysis helps by answering questions such as user-permission reachability, which asks whether specified users can together change the policy in a way that achieves a specified goal, namely, granting a specified permission to a specified user. This paper presents a rule-based access control policy language, a rule-based administrative policy model that controls addition and removal of facts and rules, and an abductive analysis algorithm for user-permission reachability. Abductive analysis means that the algorithm can analyze policy rules even if the facts initially in the policy (e.g., information about users) are unavailable. The algorithm does this by computing minimal sets of facts that, if present in the initial policy, imply reachability of the goal.

3. Andrea Margheri, Massimiliano Masi, Pugliese and Francesco Tiezzi identified that Access control systems are widely used means for the protection of computing systems. They are defined in terms of access control policies regulating the access to system resources. In this paper, we introduce a formally-defined, fully-implemented framework for specification, analysis and enforcement of attribute-based access control policies. The framework rests on FACPL, a language with a compact, yet expressive, syntax for specification of real-world access control policies and with a rigorously defined denotational semantics. The framework enables the automated verification of properties regarding both the authorizations enforced by single policies and the relationships among multiple policies. Effectiveness and performance of the analysis rely on a semantic preserving representation of FACPL policies in terms of SMT formulae and on the use of efficient SMT solvers. Our analysis approach explicitly addresses some crucial aspects of policy evaluation, such as missing attributes, erroneous values and obligations, which are instead overlooked in other proposals. The framework is supported by Java-based tools, among which an Eclipse-based IDE offering a tailored development and analysis environment for FACPL policies and a Java library for policy enforcement. We illustrate the framework and its formal ingredients by means of an e-Health case study, while its effectiveness is assessed by means of performance stress tests and experiments on a well-established benchmark.

PROPOSED SYSTEM

The proposed system uses SharePoint as its primary document repository. In SharePoint there is a built-in entity called as Document Library. This document library is used as repository for storing the documents which can be viewed by the user/creator later. The document library will have the metadata fields which will be used for storing the properties of the document and all other related data. Users will have a form which they will be using for keying the details of the policy and will upload the policy. The uploaded policy will be stored in the document library by using Microsoft Graph REST API call. Once the policy is uploaded, Power Automate workflow gets triggered and the approval process gets started. Workflow is responsible for sending email notification and updating the status of the policy based on approver input. The policy will be moved to the appropriate approvers login who decides whether to approve or reject the policy created, they can also have the capability to make the policy to be approved by some other authorized approver. Only the approver/author can view, update and delete the policy before it is fully approved and published. In case of rejecting the policy it is mandatory for the approver who rejects the policy to upload a comments for it stating the reason for rejecting it. The common users cannot have the access to view the policy which is not yet approved. Once all the policy is approved by all approvers the workflow will call the Azure Cognitive Services and pass the policy document as input to the service. The service will extract the keywords based on the defined text extraction algorithm and populate the metadata for the uploaded policy. The approved policy will also be updated in the PDF format in a common access in order to avoid unnecessary modification done in the approved policy by unauthorized users. In any case the policy owner/author can update or delete the policy which will also be updated in common access listing of all the policies created which can be viewed by common users through web application. All the updated policy in the common access were sorted in last come first in order. So the latest policy will be prioritized and viewed by the users.

CONCLUSION

All organizations have their policies created and stored at multiple places and all of them are consolidated. Thus now using this application employees can go, search and get the right policy whenever they need it. There is a rule to update the policies after a specific period every thing is a audit. If an organization is not found with an updated policy, it will be definitely fined and this software enables Automatic policy renewal. Old policies can be retrieved over a specified period of time. Updated policies are accessed efficiently. Multiple level authoring allows in multiple people approvals before publishing of the policies. The future enhancement is to automate the process of checking the policy expiry date by checking the validity time for the policy and sending an alert through mail or text to the regarding owner/author about the policy expiring state and ask them to either delete or archive or renew the process.

REFERENCES

[1] Wei zong, Freng Wu, ZhengruiJiang,"A Markov-based update policy for Constantly changing database systems", IEEE Transactions on Engineering Management Volume: 64 , Issue: 3 , Aug. 2017 .

[2] Puneet Gupta, Scott D.Stoller, ZhongyuanXu,"Abductive analysis of administrative policies in rule-based access control", IEEE Transactions on Dependable and Secure Computing Volume: 11, Issue: 5 , Sept.-Oct. 2014 .

[3] Andrea Margheri , Massimiliano Masi , Rosario Pugliese and Francesco Tiezzi,"A Rigorous Framework for Specification, Analysis And Enforcement of Access Control Policies",IEEE Transactions on Software Engineering, Volume: 45, Issue: 1 ,24 October 2017.

[4] Masoud Narouei, Hassan Takabi and Rodney Nielsen,"Automatic Extraction of Access Control Policies from Natural Language Documents", IEEE Transactions on Dependable and Secure Computing,23 March 2018 .

[5]Eiji Adachi Barbosa ; Alessandro Garcia ; Martin P. Robillard ; Benjamin Jakobus,"Enforcing Exception Handling Policies with a Domain-Specific Language",IEEE Transactions on Software Engineering,Volume: 42, Issue: 6,01 JUNE 2016.

[6]FulvioValenza; Cataldo Basile ; Daniele Canavese; Antonio Lioy,"Classification and Analysis of Communication Protection Policy Anomalies", IEEE/ACM Transactions on Networking,Volume: 25 , Issue: 5 , Oct. 2017.

[7] Yan Zhu, Ruyun Yu, Di Ma, and William ChengChungChu,"Cryptographic Attribute-Based Access Control (ABAC) for Secure Decision Making of Dynamic Policy With Multiauthority Attribute Tokens", IEEE Transactions on Reliability ,Volume: 68 , Issue: 4 , Dec. 2019 .

[8]Adrian Lara; Byrav Ramamurthy,"OpenSec: Policy-Based Security Using Software-Defined Networking",IEEE Transactions on Network and Service Management,Volume: 13 , Issue: 1 , March 2016.

[9] Amani Abu Jabal ; Maryam Davari ; Elisa Bertino ; Christian Makaya ; SeraphinCalo ; Dinesh Verma ; Christopher Williams,"ProFact: A Provenance-based Analytics Framework for Access Control Policies,"IEEE Transactions on Services Computing, January 2016 .

[10] Hui Shen, Ram Krishnan, Rocky Slavin, JianweiNiu,"Sequence Diagram Aided Privacy Policy Specification",IEEE Transactions on Services Computing, February 2019 .