Service Operation

Incident Management – Automation

Saurabh S Pisal

Department of IT & Management,

IIT Chicago  
+1 (312) 804-7225

spisal@hawk.iit.edu

**ABSTRACT**

The greatest challenge in any Workflow management system is to track down every incident that takes place. An Incident track record system should be able to adapt to the changes taking place in the organizational environment. Even authorities managing the workflow vary fundamental knowledge. A workflow model is way to deal with such scenario for Incident and Problem Management [1].

**OVERVIEW**

This paper explains ways to handle incident and problem and its proper management. A tool or rather an incident & problem management using automation will be introduced to handle and predict the incoming issue before hand.

**Keywords**

Workflow Management system; Incident handling tools; automatic decision making; data mining; Configuration Item (CI); KB Articles; Configuration Management Database

# INTRODUCTION

Any IT organization need to manage its issue related to any department be it its own IT or the client they are handling. Every department and process of the organization needs an Incident logger and Tracking system. This helps the organization to handle their cost and tackle current situations as well as make improvement plans and predictions. But for the organization to work smoothly, this incident logging tool needs to be managed properly [2].

The workforce taking care of logging INCs need to be aware of the process. Still, the organization face loss due to improper INC handling and its recovery. We are going to discuss automatic decision-making model using the technique of data mining which will further identify the affected CI’s based on the past history logs predict the INC’s classification and retrieve the Knowledge based (KB)Articles and even suggest past Incidents similar to the projected CI and Classification of INC [3]

# AUTOMATION

In order to improve the reputation of any organization user satisfaction is of higher importance and minimizing the impact occurring on business which can be achieved by restoring interrupted services. This is even accompanied by Emergency Change Management, but we are mainly concerned with Incident Management and permanent fixes for the reoccurring incidents [3]

Till now handling those incidents was taking care manually but individuals. Filtering and analyzing was done by the assigned individual to make out valuable information out of it.

Automation aims using Data-Mining technology to build an automatic decision-making model which will analyze history database of the incidents and archive the acquired knowledge in other DB which will help in auto-incident management process which further helps improving the response to new incoming INC.

1. *Stack Matching Technique*

Method designed by Brodie et al to quickly find known software issues which concentrates on feature match [4]. Its responsibility is identification of existing INC weather a common problem or not and come up with decision making support analysis [4]. This method figures out system crash causes /SI interpretation and tries to figure out the incident submitted by the Client and the history Incidents - Suggest methodologies to resolve issue accordingly

1. *Keyword Index Search*

Method proposed by R. Gupta - states use of Configuration item (CI) retrieval process which is further based on unstructured INC descriptions inputs [5]. Delivers keyword index to search for CI’s directly coming under a common list which further uses relationship index to check the CI’s and returns the Analyzed and predictive results to the Front-end user [5].

# Incident Decision-Making Model

The Incident Decision-Making Model consist of 3 methods. A. Keyword Search Engine B. Classifier C. Incident Search Engine

1. **Keyword Search Engine**
2. *Keyword Extractor*

This is the first component of keywords search engine module. It follows word segmentation as soon as the Incident description is obtained. In this noun phrases are selected, and output is produced with the most meaning full sentence derived from word segmentation [3].

In the end the keywords are matched with the dictionary and the results are outputted with the highest match from the Database of Knowledge collection (Configuration Management Database CMDB) [3]

1. *CI indexing*

CI indexing auto retrieves CMDB with respect to the input keywords and returns CI’s with most match which will be highly related to the INC hence reducing manual intervention and errors by human workflow handler (Usually L1 support but not confined to)

Incident Description

Keywords Dictionary

Keywords Extractor

CI Indexing

Key Search Engine

1. **Machine-Learning Classifier**

After processing is done in key search engine the current searched INC description is verified against a training classifier which has studied the CMDB. This machine learning classifier methodology will generate an effective model with the historic INC’s.

Key Search Engine

Classifier Engine

1. **Incident-Search Engine**
2. *Similarity Match Architecture*

In this block, the filtered CI goes further into Incident-search Engine which deploys an architecture to checking a similar match to previously known incidents. Here comes the part of Problem Management handling. Problem Management team and set their parameters here to understand and gain access to INCs which have been reoccurring.

The period and frequency of the INC comes in can be tracked on this part of the model.

1. *Similarity Match Retrieve*

This block will retrieve the data from CMDB and will produce the result out to the front end. In the end the front user will be able to compare it with actual issue and produce statistics to the team or even personal decision on working on the ticket. This method proposed can produce about 87% of accuracy and solving the INC’s with automation achieving higher decision accuracy in support, lower support cost and a higher degree of automation

Similarity match retrieve

Similarity match architecture

Incident Search Engine

Top Results

# CONCLUSION

We can construct this Automatic Decision-making model which is based on Data Mining to identify the CI’s on historical data. This identified CI’s can be used for predicting INC classifications and extract KB’s from the same. This model has helped in improving the INC management process in major aspects like - reducing the dependency on L1 support person, fault tolerant where the input description need not to be highly accurate to suggest KB articles and past reference INC’s and thirdly as the model completely utilizes the knowledge database it highly improves the response time to the Incidents and its Management like in Problem Management improves drastically.

# REFERENCES

1. L. Lema-Moreta and J. Calvo-Manzano, "A proposal for implementation of ITIL incident management process in SMEs," 2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM), Salinas, 2017, pp. 1-5. doi:10.1109/ETCM.2017.8247494
2. M. Stoute, Jiacun Wang, D. Rosca, W. Tepfenhart and A. Milewski, "Workflow Management Tool Support for Incident Command Systems," 2006 IEEE International Conference on Networking, Sensing and Control, Ft. Lauderdale, FL, 2006, pp. 703-709. doi:10.1109/ICNSC.2006.1673232
3. M. Yun, Y. Lan and T. Han, "Automate incident management by decision-making model," 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA) (, Beijing, 2017, pp. 217-222. doi:10.1109/ICBDA.2017.8078811
4. Brodie, Mark, et al. "Quickly finding known software problems via automated symptom matching." Second International Conference on Autonomic Computing (ICAC'05). IEEE, 2005.
5. Gupta, Rajeev, K. Hima Prasad, and Mukesh Mohania. "Information integration techniques to automate incident management." NOMS 2008-2008 IEEE Network Operations and Management Symposium. IEEE, 2008.