IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 10, October 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 10, October 2024

|DOI: 10.15680/IJIRSET.2024.1310052|

Secure Multimedia Data Transmission on Mobile Devices Using Real-Time Distortion Encryption and Restoration Decryption

Puneetha B H, Puneeth S P

Assistant Professor, Department of Computer Science & Business systems, Bapuji Institute of Engineering & Technology, Davangere, Karnataka, India

Assistant Professor, Department of Information Science & Engineering, Bapuji Institute of Engineering & Technology, Davangere, Karnataka, India

ABSTRACT: In the modern age of computing, it's clear that humanity has transitioned from a static to a dynamic lifestyle, with mobile devices becoming an integral part of everyday activities. Mobility now dominates our lives, making it difficult to find anyone without a mobile phone, particularly in developed and developing countries. Mobile devices primarily focus on optimizing battery usage, processing power, and memory management. However, when it comes to data security, mobile platforms still face significant challenges. While various cryptographic algorithms have been studied, most are designed with desktop applications in mind, leaving a gap in security solutions tailored for mobile devices. Well-known algorithms such as DES, AES, Triple DES, and elliptic curve cryptography require substantial computational power, which exceeds the capabilities of many mobile devices. In this paper, we focus on proposing a highly efficient, two-layered security approach, introducing 'distortion encryption' and 'restoring decryption' methods specifically for multimedia data on mobile devices, with a particular emphasis on image security

KEYWORDS: Algorithm, Encryption, Decryption, Multimedia cryptography

I. INTRODUCTION

Mobile phones are undetectable part of human beings in recent days, and they have many flaws because of their size, limited computation power, and limited battery life. So far as everyone know, at recent days android mobile phones are available in the market with some MHz (probably 500- 100 MHZ) of processing power and RAM of (100 - 400) MB with 32 GB expandable external memory slot. When these portable devices are compared with the processing power of the desktop computer (are in terms of GHz), comparison vary in big factor. So there needs to be one efficient and secure multimedia encryption and decryption algorithm for mobile devices which consumes less processing power and battery life (for ex- some of military applications require the real-time encryption of images captured from soldier's mobile phone before sending the captured image to the military repository, in order to prevent the data leakage to enemy groups) [5]. The idea involved in proposing the distortion encryption and restoring decryption is message digest algorithm, the message digest algorithm which is used in this paper is MD5[6] (the algorithm which generates Message digest is secure one-way hash function that take arbitrary-sized data and output a fixed length hash value). The MD5 hash also known as checksum for a file is a 128-bit value, something like a fingerprint of the file. There is a very small possibility of getting two identical hashes of two different files. The following figures will give the brief working procedures of the algorithms to be discussed in the later part. Following fig. 1 shows input and outputs of distortion encryption algorithm, which shows input to the algorithm is original unencrypted image and a encryption key. Output of algorithm is encrypted image

When dealing with the intricate task of analyzing process execution behavior as manifested in event logs, it is crucial to detect and address any concept drift before attempting to construct a process model or applying other process intelligence algorithms. Surprisingly, there has been limited research focused on the detection of concept drift in the context of process mining.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 10, October 2024

|DOI: 10.15680/IJIRSET.2024.1310052|

Operational processes often need to adapt to changing circumstances, whether due to new legislation, extreme fluctuations in supply and demand, or seasonal effects. When extracting a process model from event logs, the conventional assumption is that the process at the start of the recorded period remains the same as at the end of the recorded period. However, this assumption often does not hold true due to the phenomenon known as concept drift. While cases are being handled, the underlying process may undergo changes, necessitating an approach to analyze these dynamic shifts.

Our proposed approach has been implemented in ProM3 and validated through an analysis of an evolving process. In the realm of process mining, there are three primary classification techniques: Discovery, Conformity Analysis, and Extension.

Process mining is closely aligned with Business Process Intelligence (BPI), Business Operations Management (BOM), Business Activity Monitoring (BAM), and data workflow mining. The remainder of this paper is structured as follows: related work is discussed in Section II, system design is detailed in Section III, implementation is covered in Section IV, experimental results are presented in Section V, and the paper concludes in Section VI.

II. RELATED WORK

The working of above mentioned distortion encryption algorithm is depicted thoroughly in fig. 3. The inputs for distortion encryption algorithm are key from the user and original image. The following fig. 4 depicts the restoring decryption algorithm. In which original image which has been encrypted using distortion encryption will be decrypted if the message digest bytes obtained by user entered decryption key matches with the encrypted image bytes from position pdesort to Pdesort + MDlength The above working model gives the final result as encrypted image, by taking into consideration of all the available criteria, for simplicity and to keep this algorithm simple the MD5 algorithm is chosen which is simplest among all the available algorithms till now and also produces the message digest of our desired length with least programming effort, the main concept involved in this paper is to provide the security for multimedia data stored in mobile phone with utilising least power. The implemented algorithm works well with image still now further work can be carried out to extend this work towards all the available multimedia data available in these days. The byte length of message digest will provide the randomness in encryption and decryption that makes hacking the data stored in mobile is impossible, if the multimedia type ha bee encrypted using the distortion encryption and restoring decryption algorithm

Concept drift, in essence, presents a non-stationary learning challenge over time, with discrepancies between training and application data being commonplace in real-world scenarios. In this report, we address the concept drift issue in the context of process mining [3]. We introduce an ensemble method for managing concept drift, which dynamically creates and removes weighted experts in response to performance changes. This method, referred to as dynamic weighted majority (DWM), incorporates four mechanisms to effectively cope with concept drift. These mechanisms involve training online learners, assigning weights based on their performance, removing underperforming learners, and introducing new experts based on the ensemble's global performance [4].

Operational processes often undergo adjustments to adapt to changing conditions, such as shifts in legislation, significant fluctuations in supply and demand, or seasonal influences. While the topic of flexibility is well-explored in the Business Process Management (BPM) domain, contemporary process mining approaches typically assume process stability. When extracting process models from event logs, it is conventionally assumed that the process's characteristics at the beginning of the recorded period persist until the end. However, this assumption often does not hold due to the concept drift phenomenon. During case execution, the process itself may undergo changes, prompting the need for an approach to analyze these second-order dynamics.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 10, October 2024

|DOI: 10.15680/IJIRSET.2024.1310052|

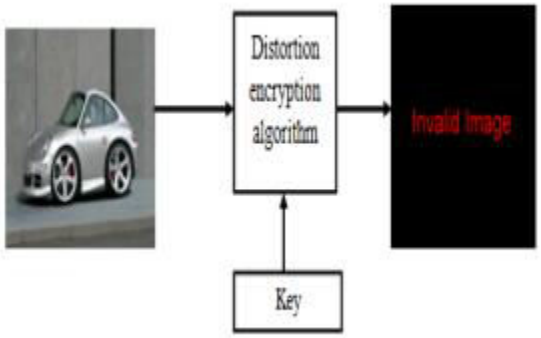

Fig. 1: Inputs and output of distortion encryption algorithm

Our proposed approach, implemented in ProM3, has been evaluated by analyzing an evolving process [5]. Decision-making in process-aware information systems involves both build-time and run-time decisions. At build-time, idealized process models are designed based on organizational objectives, infrastructure, constraints, and other factors. However, these idealized models can deviate from reality at run-time, particularly when planned activities do not occur within the expected timeframes. Users are then faced with decisions, referred to as escalations, to ensure process completion within the specified timeframe or minimize tardiness. This framework for escalations draws on established principles from the workflow management field [6].

The domain of spam filtering presents a challenging machine learning task, marked by dynamic changes in data distribution and concepts, primarily driven by spammers seeking to bypass spam filters. Lazy learning techniques are well-suited for such dynamically changing contexts. We introduce a case-based system for spam filtering that can adapt dynamically [7].

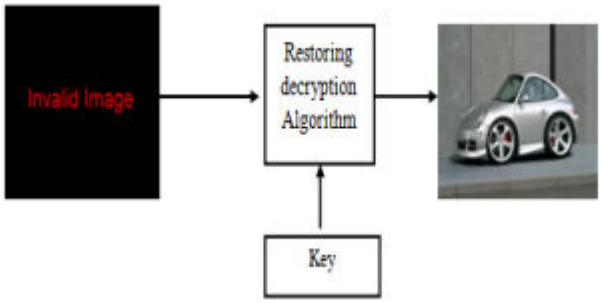

Fig. 2: Inputs and output of restoration decryption algorithm

Processes, while often similar across organizations or within the same organization, may also necessitate local variations. Configurable process models have been advocated to accommodate such variations in a controlled manner [8].

Fluctuations in fuel feeding and fuel inhomogeneity can impact the circulating fluidized bed (CFB) process, leading to efficiency reduction and shortened component lifetimes if control systems fail to compensate for these fluctuations. This paper addresses the challenge of online mass flow prediction, encompassing accurate prediction and explicit detection of abrupt concept drift, along with noise handling mechanisms [9].

Additionally, a classification and lifecycle framework for business process change is introduced to explore the influence of contextual variables on business processes and the need for different responses under varying conditions [10]. Process mining techniques play a crucial role in extracting valuable insights from event logs, including control-flow discovery, which involves the automated construction of process models to depict causal

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 10, October 2024

|DOI: 10.15680/IJIRSET.2024.1310052|

relationships between activities. These insights are pivotal for advancing the next generation of Process-Aware Information Systems (PAISs) as they highlight the disparity between proposed models and reality [11].

III. METHODOLOGY

3.1 DISTORTION ENCRYPTION ALGORITHM

The steps are as follows.
Step1: Obtain the key from the user.
Step2: Obtain the byte stream of the image.
Step3: Obtain the message digest of the key using message Digest algorithm.
Step4: Obtain the byte stream of message digest.
Step5: Calculate the number of bytes in key (position for Starting distortion) also called as Pdesort.
Step6: Insert the calculated message digest bytes from the position calculated (Pdesort) in byte stream of images.

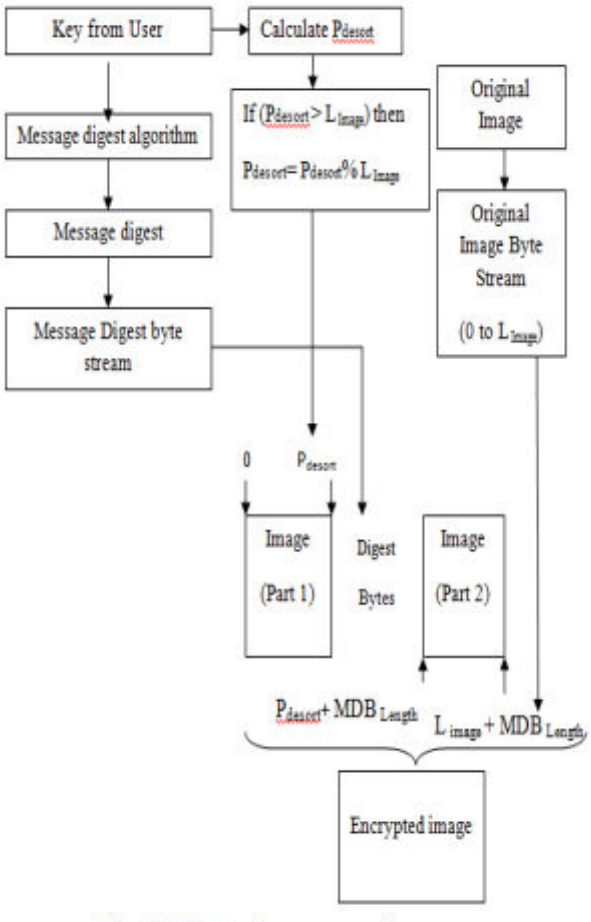

Fig. 3: Distortion encryption

3.2. RESTORATION DECRYPTION ALGORITHM

Step 1: Obtain the key from the user.
Step 2: Obtain the byte stream of the image.
Step 3: Obtain the message digest of the key using MD5 algorithm.
Step 4: Obtain the byte stream of message digest.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 10, October 2024

|DOI: 10.15680/IJIRSET.2024.1310052|

Step 5: Calculate the number of bytes in key (position for starting distortion) also called as Pdesort.
Step 6: Delete the calculated message digest bytes from the position calculated (from Pdesort to Pdesort + Message digest bytes) from byte stream of images.

1. **Environmental Monitoring:** An essential aspect of the methodology is continuous monitoring of the environment. This step involves observing and recording changes that occur within the process mining environment. These changes are a key component in detecting and understanding concept drifts.To mathematically express environmental changes

Change Rate Function: CRF(environment_variable) = Δ(environment_variable) / Δ(time)
Environmental Change Alert Threshold: T_threshold

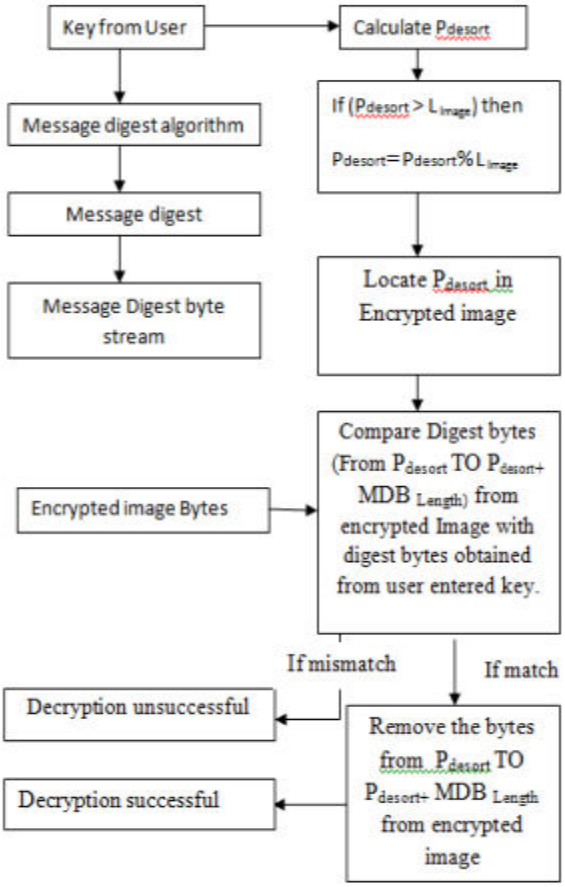

Fig. 4: Restoring decryption

2. **Event Log Recognition:** The methodology places significant emphasis on the recognition of event logs. This involves categorizing and structuring the event logs in a manner that facilitates subsequent analysis. Suitable visualization techniques are applied to make these event logs comprehensible. In this step, a mathematical representation of event log categorization can be introduced

Categorization Function: CF(event_log) = Category
Visualization Effectiveness Score: VES = (Information Captured) / (Complexity of Visualization)

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 10, October 2024

|DOI: 10.15680/IJIRSET.2024.1310052|

3. **Dynamic Analysis:** An integral part of the methodology is the dynamic analysis of the event logs. This involves utilizing the Promenade VI network to gain insights into the dynamic nature of concept drifts. The dynamic analysis is a crucial step in comprehending how the method is evolving over time.A simple mathematical model for dynamic analysis could involve:

Event Log Dynamics: EL(t) = f(t), where EL represents event log attributes and f(t) signifies how these attributes change over time.
Dynamic Analysis Metrics: DAM = (Change Magnitude) / (Change Duration)

4. **Concept Drift Identification:** The methodology is designed to facilitate the identification of concept drifts within the process mining domain. This step is achieved through the collective efforts of the four modules outlined in the framework.To mathematically identify concept drifts, you might consider:

Concept Drift Score: CDS = (Dissimilarity in Event Logs) / (Time Interval)
Concept Drift Threshold: T_CDS_threshold

IV. EXPERIMENTAL RESULTS

The proposed above algorithms are thoroughly and practically implemented and tested in mobile phone with the android operating system [7] (V 2.3 ginger bird and it is compatible with all the previous versions from 1.5 to 2.2). The proposed methods for encryption and decryption works very good with the portable devices like mobile phone with less power and time consumption. Following are some of the Results which will give the details of working and implementation of the above mentioned algorithms The pseudo code of implementation of distortion encryption is given as follows. Restoring decryption is carried in reverse steps as that of distortion encryption with some computational and implementation differences.

```
FileInputStream fis=new
FileInputStream(original image);
byte[] originalimage=new byte[fis.available()];
fis.read(originalimage);
distortion_encript(fis,key)
FileOutputStream fos=new
FileOutputStream(f);
fos.write(encriptedimage);
```

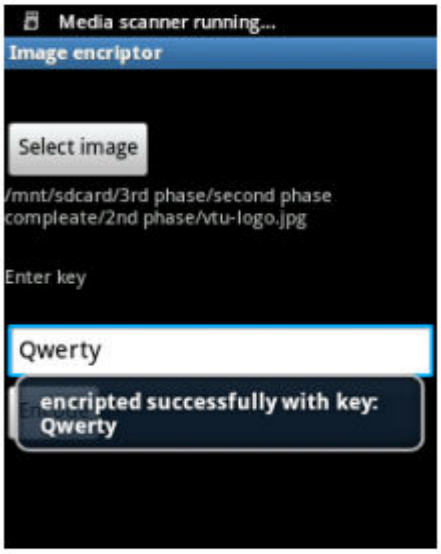

Fig. 5: Encryption UI

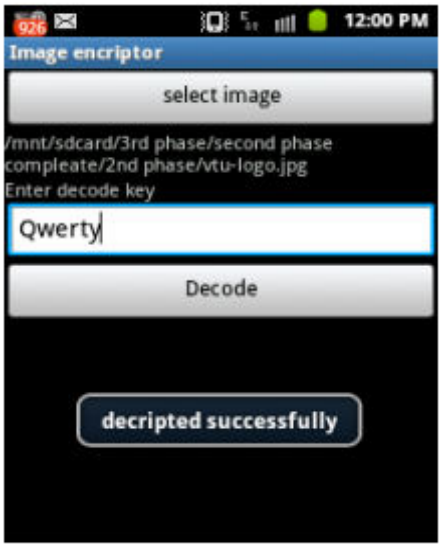

Fig. 6: Decryption UI

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 10, October 2024

|DOI: 10.15680/IJIRSET.2024.1310052|

The outcomes of addressing concept drift within the realm of process mining, utilizing event logs, are presented graphically with an X-axis and a Y-axis. This visual representation showcases the dynamics of events as they transition from one process to another, pinpointing the precise moments of change.

In Figure 2, you can observe the visualization of concept drifts. On the X-axis of the chart, we track "Change Detection Over Time," which represents the timeline of changes occurring within the process. This axis chronicles the progression of these changes.

Fig. 7: Before encryption

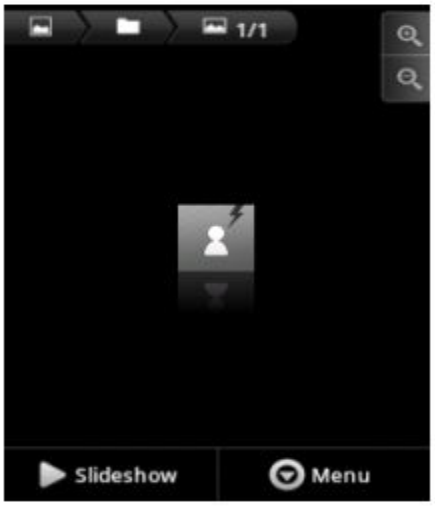

Fig. 8: After Encryption

On the Y-axis, we examine "Change Percentage," indicating the extent or magnitude of change during specific time intervals. The Y-axis values demonstrate how the level of change fluctuates, either increasing or decreasing, in response to the different event logs analyzed in the context of process mining.

This visual representation, in the form of a bar chart, provides a comprehensive overview of how the process evolves over time. It aids in the precise identification and understanding of concept drifts within the process, shedding light on how events and patterns change over time.

V. CONCLUSION

The whole summary of this work is to provide the efficient low power and low processor time consumption algorithm for encrypting and decrypting the multimedia data in mobile phone. As the proposed algorithm is simple and it works fine with the user key size of any length. The proposed algorithm provides two layers of security while decrypting, First by determining the Pdesort with user provided key. Second by comparing each bytes of the digest stored in the image with the newly calculated value of digest bytes. If there is any mismatch in digest bytes, decrypting process will be suspended. This work also shows that how to apply the proposed distortion and restoration algorithms for images. Further, this proposed work can be extended for many available multimedia types (Example- videos). This encryption decryption algorithm can be integrated with camera of mobile phone, to encrypt the images/videos captured form camera at real time before saving to phone's memory hence providing the security for data at dynamic time

REFERENCES

[1] Carmona and R. Gavaldà, "Online techniques for dealing with concept drift in process mining," in Proc. Int. Conf. IDA, 2012, pp. 90–102.

[2] B. F. van Dongen and W. M. P. van der Aalst, "A meta model for process mining data," in Proc. CAiSE Workshops (EMOI-INTEROP Workshop), vol. 2. 2005, pp. 309–320.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 10, October 2024

|DOI: 10.15680/IJIRSET.2024.1310052|

[3] I. Žliobait˙e, "Learning under concept drift: An Overview," CoRR, vol. abs/1010.4784, 2010 [Online]. Available: http://arxiv.org/abs/1010.4784.

[4] J. Z. Kolter and M. A. Maloof, "Dynamic weighted majority: An ensemble method for drifting concepts," J. Mach. Learn. Res., vol. 8, pp. 2755–2790, Jan. 2007.

[5] R.P. Jagadeesh Chandra Bose, Wil M.P. van der Aalst, Indr_Zliobait, and Mykola Pechenizkiy, "Handling Concept Drift in Process Mining", Department of Mathematics and Computer Science, University of Technology, The Netherlands.

[6] W. M. P. van der Aalst, M. Rosemann, and M. Dumas, "Deadline-based escalation in process-aware information systems," Decision Support Syst., vol. 43, no. 2, pp. 492– 511, 2011.

[7] S. J. Delany, P. Cunningham, A. Tsymbal, and L. Coyle, "A case-based technique for tracking concept drift in spam filtering," Knowl. Based Syst., vol. 18, nos. 4–5, pp. 187–195, Aug. 2005.

[8] W. M. P. van der Aalst, N. Lohmann, and M. L. Rosa, "Ensuring correctness during process configuration via partner synthesis," Inf. Syst., vol. 37, no. 6, pp. 574–592, 2012.

[9] M. Pechenizkiy, J. Bakker, I. Žliobait˙e, A. Ivannikov, and T. Kärkkäinen, "Online mass flow prediction in CFB boilers with explicit detection of sudden concept drift," SIGKDD Explorations, vol. 11, no. 2, pp. 109–116, 2009.

[10] K. Ploesser, J. C. Recker, and M. Rosemann, "Towards a classification and lifecycle of business process change," in Proc. BPMDS, vol. 8. 2008, pp. 1–9.

[11] M. Dumas, W. M. P. van der Aalst, and A. H. M. Ter Hofstede, Process Aware Information Systems: Bridging People and Software Through Process Technology. New York, NY, USA: Wiley, 2005

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details