AUTOMATIC COLLECTION AND DISTRIBUTION OF DISCOVERY TO DEFENSE ATTORNEYS

1st Foster Yeboah
Department of Computer Science
University Of Cincinnati
Cincinnati, USA
yeboahfr@mail.uc.edu

***Abstract*— The criminal justice system involves extensive paperwork, substantial documentation, and the critical need for timely information exchange among stakeholders. A key component of this process is the secure collection and distribution of discovery materials to defense attorneys. Defense attorneys must have access to all relevant evidence to provide effective legal representation, as delays or errors in obtaining discovery materials can impede their ability to prepare a robust defense. Additionally, timely access to discovery is a fundamental right of the accused, ensuring due process and a fair trial, as upheld by legal frameworks worldwide. In addressing these challenges, the integration of technology can streamline the management of discovery documents. Automating the collection and distribution of these materials not only enhances efficiency but also reduces administrative burdens, enabling legal professionals to focus on substantive tasks. This paper explores the implementation of a scripting framework within a controlled simulation to automate the secure and prompt distribution of discovery materials to defense attorneys. The system includes mechanisms to enhance cybersecurity and access control. Alerts are triggered when users attempt to access applications outside permitted hours or during system outages or maintenance. Both administrators and users are notified in such events. Additionally, a continuous monitoring script ensures user permissions are appropriately managed, preventing unauthorized access. By incorporating automated scripting, the framework aims to improve cybersecurity measures and optimize the distribution of discovery materials within the criminal justice system.**

Keywords*— *Scripting, Defense Attorneys, Distribution of Discovery, Access Control, Cybersecurity, Real-Time Responses, Suspicious User, System Insider Threats.

I. INTRODUCTION

In recent times, curbing the rising cost of civil litigation and reducing delay in case resolution have been the primary objectives of contemporary court reform. Larger proportions of judges and Attorneys have cited lawyers abuses of the discovery process. Discovery process is slow. The distribution of Discovery documents is not automatic and requires manual work from both defence and prosecution This can take weeks, thus delaying the case.

The existing literature highlights the challenges and opportunities associated with automating the collection and distribution of discovery materials in the justice's system.

The study [1], focused on finding the times and reasons attorneys neglect available discovery. The study interviewed more than three dozen Texas criminal defense attorneys and found that many of their peers fail to review discovery in felony criminal cases. The interviewees identified several explanations for the failure to access evidence. These included a lack of technological skills and support, the overwhelming volume of digital discovery, the client's desire for fast resolution of the case, the lesser gravity of some cases, high caseloads, low compensation, and in some cases, simple lack of diligence.

The study written by [2], examined the explosive growth of digital evidence in criminal cases and the efforts to manage its challenges. She reiterated that more detailed rules are crucial for effective management of Digital Discovery.

Our research looks at Automating the collection of Discovery documents related to a case and automatically distributing them to Defense Attorney on file. To address the challenges and capitalize on the benefits identified in the literature, an Information Technology (IT) solution is essential. There are some key IT issues that need consideration in this system even as we design a framework. Namely, data security, protecting sensitive legal information, is quite important. Implementing robust encryption, access controls, and secure transmission methods are all key components that need to be integrated into our proposed solution.

Secondly, the team would need to look at Standardization, establishing standardized formats for discovery materials ensure compatibility and consistency in processing and distribution.

II. RELATED WORK

The criminal justice system is known for its substantial paperwork and the importance of timely information sharing. The efficient distribution of discovery materials to defense attorneys is crucial for ensuring fair trials and upholding justice. The conventional way of managing and sharing discovery materials has been linked to inefficiencies and delays [7]. Consequently, there is an increasing demand toward incorporating technological solutions to streamline these procedures.

The study talks about evolutionary timetrees where emphasis was on manual process of finding articles containing timetrees. The study explored the effectiveness of text-mining approaches and developed optimizations to find research articles containing timetrees automatically [9].

979-8-3315-2096-0/25/$31.00 ©2025 IEEE

The incorporation of technology in the legal system has garnered considerable attention, especially concerning the automation of legal procedures [8]. Automation has the potential to streamline administrative tasks, enhance efficiency, and improve access to critical information in the criminal justice system [3].

The justice sector has observed an increasing adoption of automation to streamline administrative functions and bolster the overall efficacy of legal operations [1][4]. There is a massive outcry to implement automation initiatives across various aspects of the legal system, encompassing document management, case analysis, and evidence presentation in courtrooms. These endeavors when undertaken will significantly minimize manual efforts and enhance the precision and speed of legal processes.

The punctual and precise sharing of discovery materials to defense attorneys is critical for delivering competent legal representation. Some few drawbacks such as delays or alterations in receiving these materials can hinder the ability to construct a strong defense and may influence the final verdict of legal proceedings [1].

Discovery plays a crucial role in legal processes, providing defense attorneys with access to vital evidence required for submitting a robust defense strategy [2][7]. Any delay or error in the distribution of discovery materials can potentially impede the preparation of a comprehensive defense approach, thereby affecting the overall outcome of the legal process and potentially infringing upon the defendant's rights [2][6].

The integrating of automated scripting frameworks into the criminal justice system can significantly contribute to enhancing security and regulating access to sensitive information. Automation offers a more efficient and secure approach to managing access to crucial documents and maintaining a robust security posture within the legal landscape [3][7].

The automated scripting frameworks serve as a valuable tool for managing access to sensitive legal documents and controlling user permissions within the criminal justice system. These frameworks ensure secure and immediate access to critical information while upholding stringent access controls to safeguard the confidentiality and integrity of legal proceedings [5][10].

Since the introduction of automation holds the potential to enhance efficiency within the legal system, it also presents challenges concerning data security, user access, and system maintenance. A comprehensive understanding of these benefits and challenges is crucial for the successful integration of automated systems within the criminal justice systems framework [5][10].

The incorporation of automated scripting frameworks offers various advantages to the legal system, including enhanced data security, streamlined workflows, and improved access controls; it also introduces complexities in its delivery and potential cybersecurity vulnerabilities. Furthermore, addressing these challenges is essential to ensure the effective deployment and sustainable operation of automated systems within the criminal justice landscape [8].

III. METHODOLOGY

A. Technology Used

The following technologies were used, namely, Linux Operating system (University of Cincinnati Sandbox), Shell scripting, cronjobs, Firewalld, sshd, amba, Apache httpd and then Access Control mechanisms to ensure the automation of the collection and distribution of discovery materials.

B. Solution Description

The team will propose a solution that involves implementing an automated system using Linux Operating system, access control, cronjobs, and scripting to collect and distribute discovery materials to defense attorneys automatically. This system will ensure that the process of collecting and distributing discovery is achieved in a timely and secure manner relevant to case information.

C. Development Process

The team will start the developmental process by initially setting up a Linux-based server which will be implemented on University of Cincinnati Sandbox, another stage of the developmental process is the creation of a script that would be used for automated data collection, and the configuration of access controls to ensure data security by installing firewalld. Lastly, this process will then go into a form of testing in a controlled environment that will ensure all the parameters work effectively and improve system reliability.

The team will use Linux Operating system as a platform for this project to create users and group policies to control access to discovery materials. Some of the users that will be created are Prosecutors, Attorneys and Clients. We will also identify and manage processes and services running on a Linux system using ps and top commands. The team installed some Services like Network Service, that provides network communication for the system, sshd provides secure access to the command shell from a remote computer, firewalld provides packet filtering for security, samba provides file sharing over a network connection, Apache (httpd) provides Web communication over http protocol. The services will then be controlled through a subsystem known as system. When the system boots, systemd will call unit files to start services. The unit files act as small applications that start the processes related to the services installed. Services are only one type of unit file that is controlled by systemd. The systems administrator can manually control services through a systemd command “systemctl”. The systemctl command will be able to start, stop, restart, enable, and disable services as needed. The team will also use this command to find information about the services installed on our system. We will then run the following command to view services currently installed on the system systemctl list-units --type service. The team will then create a Bash script to complete a task, automate a task to run on a schedule with cronjob and describe target levels and what they are used for.

D. Proposed Framework

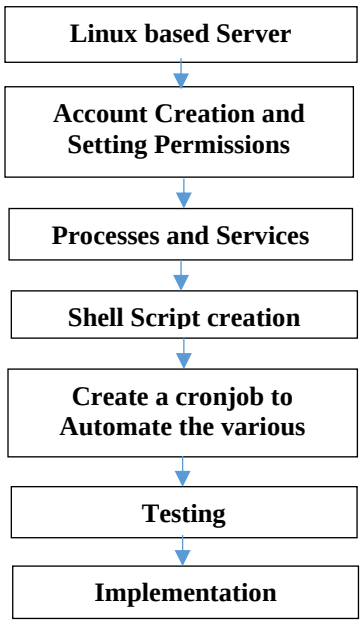

Fig. 1. Proposed Framework

E. Feasibility and Cost Estimate

The system will use a cost-effective approach which is leveraging on open-source technologies. Linux operating system is an open-source operating system and highly secure. The cost estimate could be generated from initial setup expenses and maintenance. This technology is cost effective compared to others.

F. System Development

Creating Users and Groups

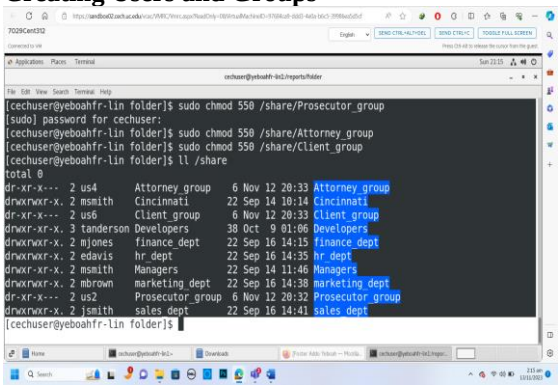

Fig. 3. Users and group creation

Users in each group can only read and execute. Everyone else cannot read, write or execute.

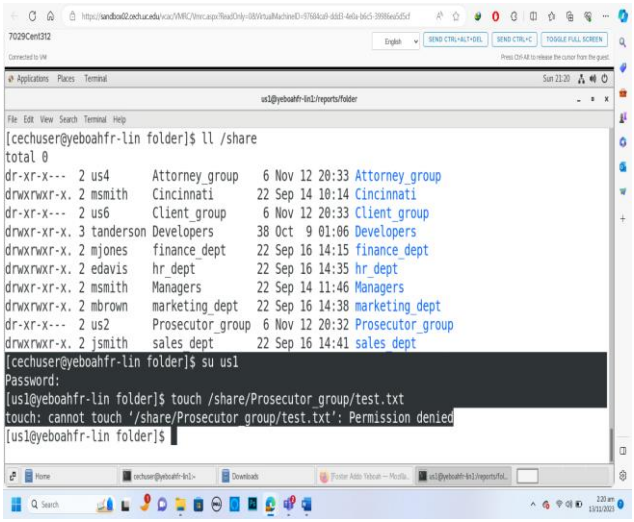

Fig. 2. Authentication

In the above screenshot, the team tried to create a file test.txt but was denied. This is because the user one (us1) only has read and execute permission.

Using Crontab

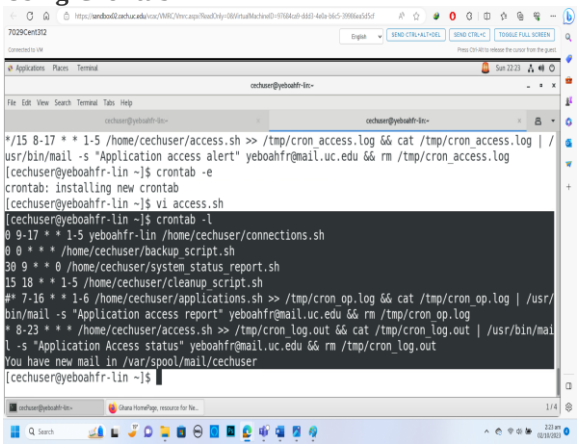

Fig. 4. Using crontab

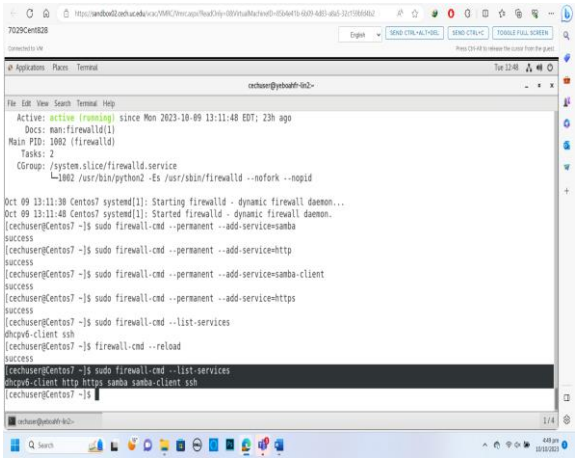

Fig. 5. Services creation

The screenshot above shows installation of firewalld services, dhcpv6-client, http, https, samba, samba-client and ssh.

IV. RESULTS

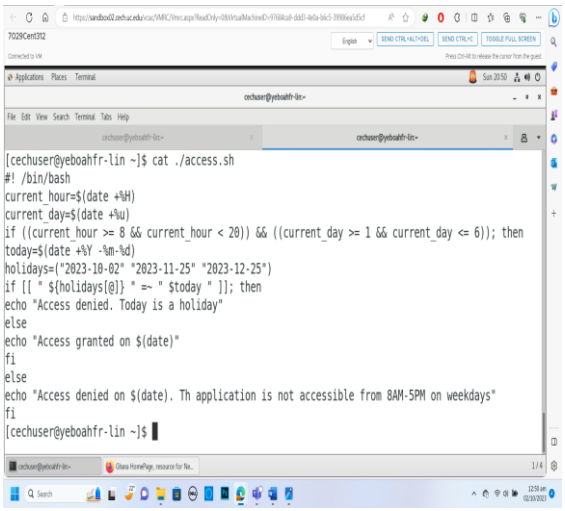

Fig. 6. Access denied

In the above script, Access will be denied when someone tried to access the system during a holiday as indicated in the script.

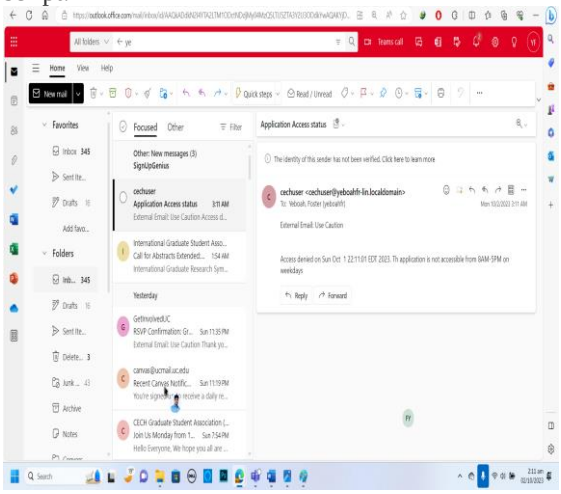

Fig. 7. Access denied

Access denied for unauthorize access. This mail is sent to the System Administrator indicating someone has been denied access.

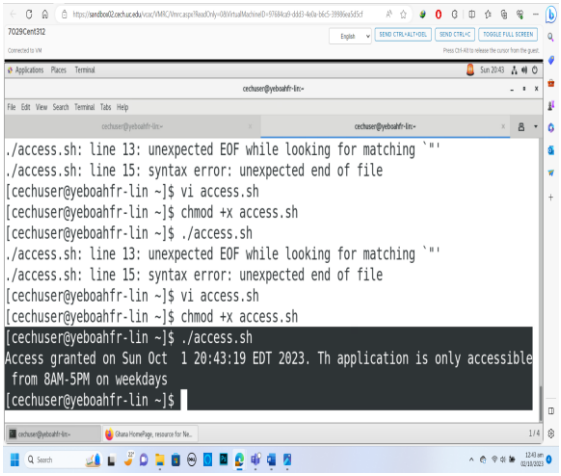

Fig. 8. Access granted

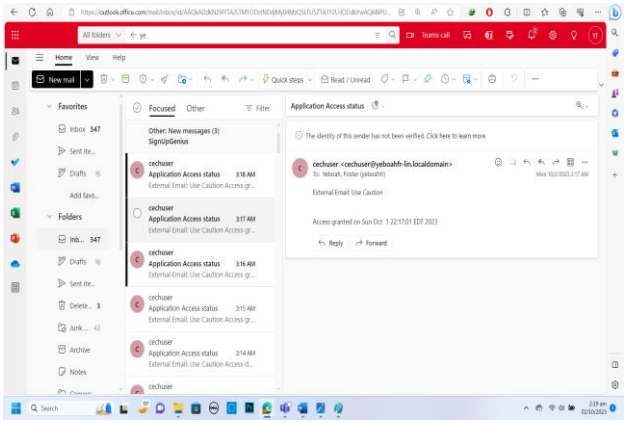

Fig. 9. Access granted

Access granted for Authorized Access. This mail is sent to the System Administrator or the one in charge if someone has been granted access to a file.

A. *Performance Evaluation*

The metrics below were used to assess the performance of the system.

Success Rate= (Total Executions/Number of Successful Executions) ×100
Error Rate= (Total Executions/Number of Errors) ×100
Script Execution Time is the total time taken by the script to complete its execution.
Delay=Script Completion Time−Script Start Time
False Positive Rate= (Total Positives/Number of False Positives) ×100
False Negative Rate= (Total Negatives/Number of False Negatives) ×100

TABLE 2. PERFORMANCE EVALUATION

Script Name	Success Rate	Error Rate	Script Execution Time	Delay	False Positives	False Negatives
Unauthorized access Alert	1	0	0.02 Secs	0 Secs	0	0
Authorized Access Alert	1	0	0.02 Secs	0 Secs	0	0

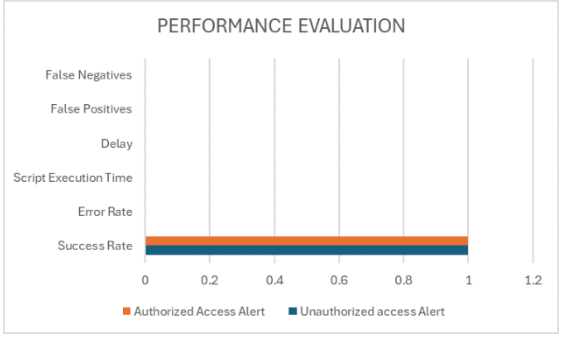

Fig. 10. Performance Evaluation

V. DISCUSSION

The response rate for both authorized and unauthorized success alerts was highly effective. The graph indicates a low error rate, demonstrating strong reliability. The script execution time was 0.02 seconds, with no noticeable delay (0 seconds) for both types of alerts. Additionally, the occurrence of false positives and false negatives was minimal for both actions, ensuring accuracy in the system's performance.

A. Issues Encountered

The team encountered a few challenges during the development stage, this has to do with script compatibility and coming out clearly with the tasks and policies related to the Client, Prosecutor and Attorney.

B. Issues Resolved

The team addressed these challenges by modifying our permissions and scripts. There were some collaborative efforts from stakeholders as well.
The proposed system will have significant impact on the efficiency of discovery distribution, enhancing collaboration between Prosecutors, Defense Attorneys and their Clients.

VI. CONCLUSION

In conclusion, automating the collection and distribution of discovery materials to defense attorneys plays a critical role in upholding justice and ensuring fair trials. Implementing an IT solution, such as the proposed framework, streamlines this essential process, enhancing the efficiency of legal procedures and benefiting both legal professionals and the broader criminal justice system.

The framework prioritizes data security, standardization, and user experience, which are vital for its successful implementation. By integrating automated scripting, the system ensures the timely and secure delivery of crucial information to defense attorneys, safeguarding the rights of the accused and reinforcing due process. This approach has the potential to significantly transform the legal domain, improving procedural efficiency while maintaining fairness and security within the justice system.

ACKNOWLEDGEMENT

I would like to acknowledge Dr Michelle Encalada and Corbin Eilmes for their contribution and support during the writing of this paper. I would like to extend our gratitude to the editors and reviewers.

REFERENCES

1. Ryan, W. (2022). Defining legal technology and its implications, International Journal of Law and Information Technology, Volume 30, Issue 1, Pages 47–67, https://doi.org/10.1093/ijlit/eaac005.
2. Vredeveldt, A., van Rosmalen, E. A. J., van Koppen, P. J., Dror, I. E., & Otgaar, H. (2022). Legal psychologists as experts: guidelines for minimizing bias. Psychology, Crime & Law, 30(7), 705–729. https://doi.org/10.1080/1068316X.2022.2114476
3. Geya Feng, Yongbin Qin, Ruizhang Huang & Yanping Chen. (2023) Criminal Action Graph: A semantic representation model of judgement documents for legal charge prediction. Information Processing & Management 60:5, pages 103421.
4. Kayes, A. S. M., Kalaria, R., Sarker, I. H., Islam, M. S., Watters, P. A., Ng, A., Hammoudeh, M., Badsha, S., & Kumara, I. (2020). A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues. Sensors, 20(9), 2464. https://doi.org/10.3390/s20092464.
5. Hugo M, et al. (2024). Textual similarity for legal precedents discovery: Assessing the performance of machine learning techniques in an administrative court, International Journal of Information Management Data Insights, 10.1016/j.jjimei.2024.100247, 4, 2, (100247),
6. Christopher A.S. (2020). Disruptive Legal Technology, COVID-19, and Resilience in the Profession
7. ABBE R. G. (2016). Unorthodox Civil Procedure: Modern Multidistrict Litigation's Place in the Textbook Understandings of Procedure
8. Nicolas K et al. (2021) The Rocket Docket System: A Model for Active Case Management in Countries Facing Judicial Delays
9. Marija, S et al. (2023). Discovering research articles containing evolutionary timetrees by machine learning, Bioinformatics, Volume 39, Issue 1, January 2023, btad035, https://doi.org/10.1093/bioinformatics/btad035
10. Yeboah F et al., "Automated Scripting for Real-Time Responses to Suspicious User Actions," (2024). IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI), Mt Pleasant, MI, USA, 2024, pp. 1-6, doi: 10.1109/ICMI60790.2024.10585642.