Enhancing Metaward: Integrating Digital Forensic Readiness in the Metaverse

Shelley M. Robertson, Stacey O. Baror and Hein S. Venter
University of Pretoria, South Africa

shelley.robertson@tuks.co.za
stacey.baror@up.ac.za
hein.venter@up.ac.za

Abstract: As virtual currencies gain traction as rewards and with the evolving landscape of remote and hybrid work environments, the need for adaptive and comprehensive reward systems becomes imperative. This research builds upon the foundation laid in prior studies, focusing on the integration of Digital Forensic Readiness (DFR) into the Metaward reward model, within the Metaverse. However, as more individuals engage with and use the Metaverse, it is crucial to implement DFR to the Metaverse. The problem of this research is the absence of DFR processes integrated into the Metaverse, particularly within the context of the Metaward reward system. With the increasing importance of cybersecurity and digital forensics (DF) in organizational operations, the integration of such measures aims to enhance the security and integrity of the Metaward model. This enhancement aims to ensure a proactive and effective response to potential security incidents, while maintaining the integrity of digital evidence. This research employs a comprehensive methodology, encompassing literature review, analysis of DF measures, and the development of an extended conceptual model. By considering factors such as the security implications of virtual currencies, incident response capabilities, and proactive DF measures, the study seeks to provide insights into the feasibility and effectiveness of this augmented reward model. The proposed model acknowledges the significance of balancing motivation and engagement with the imperative need for robust DFR. It explores potential synergies between these seemingly different elements, aiming to create a reward system that not only motivates employees but also ensures the resilience and security of the organizational digital infrastructure. This study's findings hold promise for organizations navigating the complex terrain of modern work paradigms, offering a strategic approach to bolstering employee motivation, engagement, and DFR. The conclusion reflects on the implications of the proposed integration and outlines avenues for further research in the dynamic intersection of virtual currencies, reward systems, and DF.

Keywords: Digital Forensic Readiness, Digital Security, Metaverse, Virtual Currency, Employee Motivation.

1. Introduction

The Metaverse, a dynamic fusion of virtual reality (VR), augmented reality (AR), and immersive technologies, has soared in prominence since Facebook's rebrand to "Meta Platforms" in 2021 (Roose, 2021). With the firm resolve of Meta to propel its evolution, this shared virtual space has ignited fascination and excitement, anticipating a new era of digital interconnectedness and exploration (Robertson et al., 2024; Roose, 2021).

In a previous study, Robertson et al. (2024) explored the efficacy of virtual currencies in reward systems, analysed existing reward mechanisms, and proposed a conceptual model for evaluating the feasibility of the Metaward model. Metaward is a virtual currency reward system that offers a holistic framework aimed at revitalizing employee motivation and engagement in the Metaverse. By combining rewards, penalties, recognition, and social comparison, Metaward cultivates a dynamic workplace environment adaptable to align with the mission and values of an organization. This versatile approach holds the promise of substantially boosting employee performance and job satisfaction.

However, amidst the transition to virtual reward systems, the study identified a crucial gap in ensuring the security and integrity of the Metaward model against potential cyber threats. Integrating Digital Forensic Readiness (DFR) into the proposed Metaward model, within the Metaverse, is a critical evolution necessitated by the adoption of virtual currencies as rewards and the imperative to fortify organizational resilience against cyber threats.

The field of digital forensic (DF) science is in constant evolution, employing diverse scientific principles to improve digital evidence and data recovery (Baror and Venter, 2013). DF involves a methodical approach to examining digital data, employing advanced mathematical algorithms to uphold the integrity and trustworthiness of the information (Muyambo and Baror, 2023). Establishing a DF framework is crucial, as neglecting to do so can result in significant time and resource expenditure during the DF procedure (Nugroho et al., 2023). A DF framework is a procedural model or methodology guiding the investigation process, defined as a structured set of stages emphasizing specific phases of DF, including identification, collection, preservation, and examination analysis (Kristyan et al., 2020). This ensures a suitable level of proficiency to preserve, gather,

safeguard, and analyse potential digital evidence, enabling its effective utilization in various contexts, such as legal proceedings, security inquiries, disciplinary actions, employment tribunals, or court proceedings (Watson et al., 2018).

DF methodology branches into two categories: proactive and reactive. Reactive DF involves investigating events retrospectively, conducting postmortems, analysing behaviour, and documenting lessons learned to prevent future occurrences. On the contrary, proactive (forensics readiness) entails preparatory measures implemented before an incident arises (Kristyan et al., 2020). Incorporating DF capabilities into Metaward may enhance security, ensure compliance, provide valuable insights, and support investigations, ultimately contributing to the effectiveness and trustworthiness of the reward system.

The objectives of the DFR process aim to maximize the effective utilization of digital evidence, reduce investigation costs, mitigate interference with and prevent disruption of business operations, and maintain or enhance the existing level of information systems security (Valjarevic and Venter, 2012). DFR involves establishing a genuine, resilient, and transparent auditing mechanism in anticipation of potential digital investigations (Muyambo and Baror, 2023). It encompasses an organization's preparedness to conduct DF, allowing for the optimization of investigative capabilities using digital evidence while minimizing the associated costs and time (Nugroho et al., 2023).

The convergence of virtual currencies as rewards in the Metaverse and the imperative to safeguard against potential security breaches underscores the critical need for proactive measures to detect, respond to, and mitigate security incidents. By incorporating DFR principles and practices into the Metaward model, organizations are able to fortify their defences, bolstering resilience against cyber threats, and ensuring the integrity and trustworthiness of the Metaward model.

However, it is unclear how to incorporate robust DFR into the Metaward model. This provides an opportunity for the researcher to explore the integration of DFR into the Metaward model, aiming to bolster security, ensure compliance, offer valuable insights, and facilitate investigations. The objectives of the research include: 1) A literature review on existing DFR implementations. 2) An analysis of existing models, adapting them for the Metaward model. 3) Developing a conceptual model and evaluating the research's validity.

To accomplish this objective, an extensive literature review entails exploring the ACM Digital Library Full-Text Collection, IEEE Xplore Digital Library, and ScienceDirect databases, from 2018-2024, yielding 104 research articles. The research employs a three-step methodology, as outlined by Keshav and Cheriton (2007), to sift through and pinpoint pertinent articles. Additionally, references from selected papers are considered to bolster the research's scope and depth. The process concludes with the creation of an inventive conceptual model, which encapsulates the fundamental elements of the research.

The objective of this research is to strengthen the Metaward model through the integration of DFR to enhance security measures. Through the systematic integration of DFR, this study ensures the reliability of Metaward and maintains the intrinsic benefits of the model, which utilizes virtual currencies to foster employee motivation and retention.

The subsequent sections of this paper are organized as follows: Section 2 provides an overview of prior research concerning the Metaward model. Section 3 presents the background literature relevant to the study. Following this, Section 4 introduces the proposed conceptual model. Section 5 illustrates case scenarios that underscore the contributions of the conceptual model. Section 6 discusses related literature, comparing it with the proposed model. In Section 7, an evaluation of the proposed conceptual model is presented. Finally, Section 8 concludes the work and outlines avenues for future research.

The following section encompasses the preceding research for this study.

2. Overview of Related Literature

This section comprises three subsections. Subsection 2.1 presents the literature review, where DFR implementations are examined to identify fundamental concepts, adaptable frameworks, and pertinent security insights applicable to the research. Subsection 2.2 delves into related literature, illuminating both alignments and divergence between the existing literature and the present study. Finally, Subsection 2.3 offers an overview of the authors' previous work, contextualizing their contributions within the broader scope of the study.

2.1 Literature Review

The literature review subsection is divided into four distinct areas of focus, revealed by the literature. These include insider threats, secure storage of digital evidence, privacy protection, and forensic-ready software systems. This division enhances clarity and facilitates focused discussion on each topic.

2.1.1 Insider Threats

The threat of a cyberattack looms over virtually all digital systems. These attacks are executed by diverse actors with varying objectives, expertise, and resources. Among these, a distinct category involves insider actors, who possess intimate familiarity with the system and lawful access to its resources. Consequently, malicious insiders are at an advantage in executing successful attacks and evading detection, by circumventing security protocols. Furthermore, unintentional insiders may, inadvertently, introduce exploitable vulnerabilities due to errors, oversight, or neglect (Daubner et al., 2023).

Mitigating cyberattacks originating from insiders, proves challenging with conventional security approaches. Often, such perpetrators leverage authorized system access to execute an attack, or external intruders assume an insider's identity, to breach security measures. One potential solution is the adoption of forensic-ready software systems, which facilitate comprehensive forensic investigations post-incident. These systems ensure the generation and accessibility of pertinent evidence, in the event of an attack. While not focused primarily on prevention, the controls inherent in forensic-ready systems, serve to bolster effective post-incident scrutiny, particularly in cases of insider threats (Daubner et al., 2023).

Daubner et al., (2023) propose a systematic strategy for tackling insider attacks within software systems, by integrating forensic-ready features. Essentially, this approach aims to facilitate investigations into attacks carried out or facilitated by insiders. To achieve this goal, the authors devise a risk management framework for forensic readiness, an extension of Information Systems Security Risk Management (ISSRM), which aids in crafting software systems ready for forensic analysis. Consequently, the concept of forensic readiness is seamlessly integrated with security measures, addressing vulnerabilities, and harmonizing the two aspects.

2.1.2 Secure and Transparent Storage of Digital Evidence

Xiao et al., (2024) introduces a novel DF framework, which leverages blockchain technology for Industrial Internet of Things (IIoT) environments. The framework utilizes blockchain to ensure the secure, immutable, and enduring storage of digital evidence. Addressing the real-time requirements of IIoT, it also introduces an efficient batch consensus mechanism. Furthermore, the framework incorporates token-based authorization, for controlling access to evidence queries and facilitates swift retrieval, through smart contracts. It employs public key cryptography to safeguard device identities' anonymity and ensure the confidentiality and integrity of data transmission. However, it is important to note that the framework has only undergone testing in limited simulated environments, and further refinement is necessary before its deployment in real-world industrial network scenarios.

Singh et al., (2022) introduces a model and platform designed to secure Potential Digital Evidence (PDE) and ensure its forensic integrity. Through evaluation, the platform demonstrates strong performance, successfully navigating all forensic processes outlined by the proposed model (SecureRS). Establishing a process to secure evidence, aids in preventing unauthorized access, and ensures compliance with regulations and privacy policies. Additionally, the model facilitates verification, validation, and admissibility of stored PDE in legal proceedings. Leveraging encryption and hashing, the SecureRS model, adheres to current security standards, enhancing forensic investigations, and aiding in detecting evidence tampering. The paper suggests a method for ensuring forensically sound digital evidence, addressing an aspect often overlooked, and typically deemed the sole responsibility of forensic investigators. Additionally, the SecureRS platform serves as a secure backup for evidence, alleviating concerns about verification and authenticity during digital investigations.

2.1.3 Privacy Protection in Digital Forensics

Ogunseyi and Adedayo (2023) explores cryptographic techniques for privacy protection in DF, analysing relevant studies that have utilized such techniques. It summarizes findings from each study, identifies drawbacks of cryptographic techniques in privacy protection, and suggests potential solutions. Additionally, it proposes a conceptual model for privacy-preserving DF, based on cryptographic techniques, detailing where each encryption method can be applied within the model. The study provides mathematical representations and

algorithms for the model, evaluates its performance against identified analysis factors, and considers situational factors at each stage. It compares the model with existing privacy preservation principles in DF investigations, offering a roadmap for investigators and researchers. Evaluation of the conceptual model demonstrates its alignment with key privacy principles and adaptability to various DF scenarios.

2.1.4 Forensic-Ready Software Systems

Kwon et al., (2019) posits that cyberattacks targeting financial networks, are increasingly sophisticated and severe, with frequent reports of major hacking incidents. The Bangladesh bank robbery case underscored the crucial role of DF evidence. Therefore, in incident response, effective DFR with comprehensive information is imperative. To enhance DF capabilities, Kwon et al., (2019) proposed employing IP traceback, with server marking techniques, to enable the collection of attacker information. Additionally, visualization techniques for the FIX protocol, facilitate the investigation of large volumes of FIX network data. The FIX protocol facilitates the trading of financial products, such as stocks and cryptocurrencies.

Pasquale et al., (2018) examines the concept of forensic readiness in software systems, and the necessary requirements to achieve it. Data-centric requirements identified include availability, relevance, minimality, linkability, completeness, and non-repudiation. Process-centred requirements focus on data provenance and legal compliance. The study also outlines some open software engineering challenges in this area. For future research, the authors plan to formally characterize forensic readiness requirements, and explore techniques, for quantitatively analysing trade-offs between conflicting requirements. They also aim to investigate aspects related to implementing a forensic-ready system, such as generating specifications or assessing the relevance of preserved data.

Rivera-Ortiz and Pasquale, (2019) introduce a novel approach to automate the development of forensic-ready software systems, pioneering the automated generation of logging instructions, to cover relevant security incidents. The authors plan to develop a tool implementing three stages: Incident Modelling, Logging Instrumentation, and Logging Generation. They anticipate Incident Modelling and Logging Instrumentation to be particularly challenging, involving the instrumentation of software system components, to detect method execution, and annotation of sequence diagrams, with logical constraints. The Logging Generation stage is to include the addition of an engine to generate alerts and analyse log messages, potentially encrypting them for enhanced security. Consideration is also given to privacy concerns and strategies, to minimize excessive logging.

2.2 Related Literature

Integrating DFR into Metaward is crucial given the diverse challenges, including insider threats, secure storage of digital evidence, privacy protection in DF, and sophisticated cyberattacks on financial networks. DFR measures address these challenges by providing a systematic strategy for preparatory measures to be implemented before an incident arises, ensuring transparent storage of digital evidence, safeguarding privacy through cryptographic techniques, and enhancing incident response capabilities.

The integration of DFR within Metaward is strategically aligned with the best practices gleaned from the comprehensive literature review. This integration bolsters the system's capacity to withstand the ever-changing landscape of cybersecurity threats by ensuring proactive measures are in place to detect, respond to, and recover from potential incidents effectively.

The comparison presented in Table 1 provides insights that inform the incorporation of DFR, ensuring that Metaward remains robust, adaptive, and equipped to address emerging challenges while upholding the highest standards of security and integrity.

Table 1: Related Literature comparison

Reference	Related Literature	Current Literature	Main Difference/ Contribution
Daubner et al., (2023)	Highlight the need for forensic-ready features to address insider attacks in software systems.	Integrate DFR into Metaward to facilitate investigations into insider threats.	Implementation of DFR into a specific reward system context.
Kwon et al., (2019)	Address cyberattacks targeting financial networks and propose techniques to enhance forensic capabilities.	Incorporate IP traceback/FIX protocol in Metaward to enhance DF capabilities.	Application of forensic techniques for incident response in a specific reward system context.

Reference	Related Literature	Current Literature	Main Difference/ Contribution
Pasquale et al., (2018)	Examine forensic readiness requirements in software systems, detailing datacentric and process-centred requirements.	Integrate DFR principles into Metaward, ensuring system readiness for forensic analysis.	Focus on implementing DFR principles for comprehensive forensic analysis in a specific reward system context.
Rivera-Ortiz and Pasquale, (2019)	Introduce automated logging instruction generation for forensicready software systems.	Emphasize event logging and secure off-site data storage in Metaward, indicating a shared interest in automating forensic tasks.	Automate event logging and securely store logged/alert data for a specific reward system.
Ogunseyi and Adedayo, (2023)	Examine cryptographic techniques in DF for privacy protection, offering a model and roadmap.	Highlighting secure log transmission and privacy in Metaward demonstrates cryptographic awareness.	Emphasize privacy measures and cryptographic techniques in a reward system context.
Singh et al., (2022)	Present the SecureRS model and platform for securing PDE with strong forensic integrity.	Advocate for SecureRS model in Metaward, showing a joint commitment to forensic data integrity.	Application of SecureRS model recommendation in a specific reward system context.
Xiao et al., (2024)	Introduce a blockchainbased DF framework for IIoT, highlighting interest in secure evidence storage.	Highlight secure log transmission in Metaward, aligning with digital evidence integrity.	Focus on secure log transmission and off-site storage in a specific reward system context.

The following subsection expands on the authors' previous work conducted, relating to this study.

2.3 Authors' Previous Work Related to Current Study

Robertson et al. (2024) delve into the evolving landscape of virtual work environments, particularly in the context of the Metaverse, where virtual currencies are increasingly utilized as rewards in virtual environments. With a focus on employee motivation and retention, the study addresses the gap in understanding how virtual currencies can effectively function within reward systems, in the Metaverse, and their impact on employee engagement. Through a comprehensive review of literature, the paper explores existing reward mechanisms (Christy and Fox, 2014; Farzan et al., 2008; Pombo et al., 2019; Pombo and Santos, 2023), considerations of social comparison (Christy and Fox, 2014; Dong and Zhu, 2023) and loss aversion (Lin et al., 2023), and the integration of blockchain technology for security.

A conceptual model, the Metaward reward model, is proposed, incorporating elements of rewards, penalties, recognition, and social comparison to create a dynamic and motivating environment for employees. This model offers flexibility in reward options and aims to increase productivity and job satisfaction in virtual workspaces. A proof of concept demonstrates the practical implementation of the Metaward model, highlighting its potential effectiveness in motivating and retaining employees.

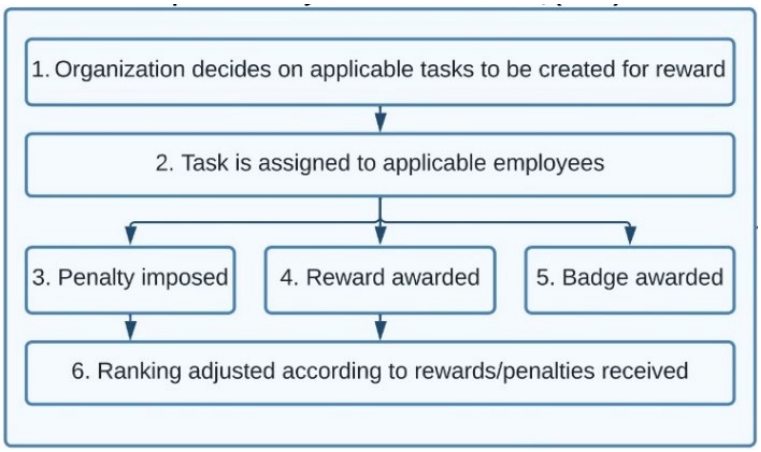

Figure 1: Conceptual Metaward model (Robertson et al., 2024)

The conceptual model presented in Figure 1 outlines a systematic approach to task, integrating various components to optimize employee engagement and performance. Tasks or challenges are meticulously generated and reviewed to align with organizational requirements. Once approved, tasks are assigned to employees with specified deadlines and notifications, with periodic reminders incentivizing timely completion.

Failure to meet deadlines incurs cryptocurrency penalties, while successful completion earns employees' cryptocurrency rewards, which can be redeemed through various options. Additionally, badges are awarded for completed tasks to foster social comparison among employees, with rankings fluctuating based on task completion status. This comprehensive model effectively combines task management strategies with motivational incentives to drive employee productivity and achievement.

In conclusion, the paper presents a promising approach to address the challenges of virtual work environments, offering valuable insights and practical strategies for organizations seeking to optimize employee performance and satisfaction in the Metaverse.

The subsequent section delves into the Metaward model with DFR included.

3. Proposed Metaward Model Including Digital Forensic Readiness

In this section, DFR is introduced into the existing Metaward model, expanding upon the discoveries from the preceding section. It encompasses a conceptual model, flow diagrams for individual components, and an overarching model flow diagram. The figure below represents the high-level conceptual model, elaborated on in section 3.1:

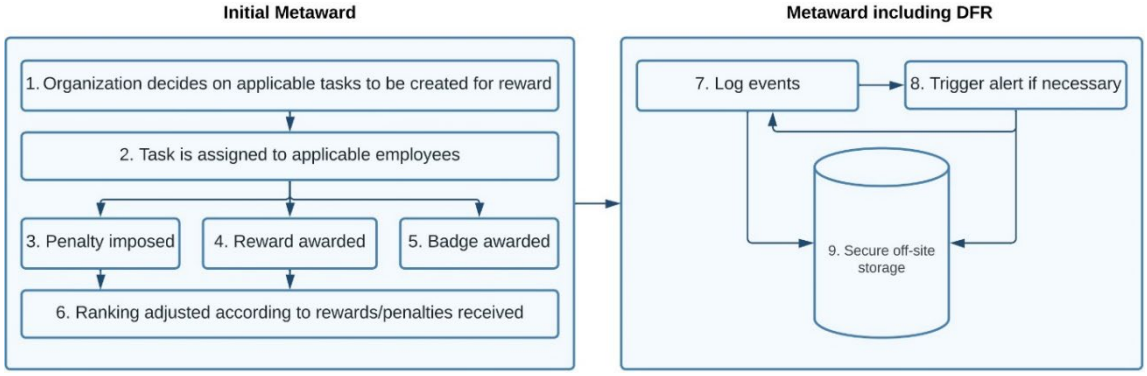

Figure 2: Conceptual Metaward model (Robertson et al., 2024) including Digital Forensic Readiness

3.1 High-Level View of Proposed Digital Forensic Ready Metaward Model

Outlined below are the components of the conceptual model depicted in Figure 2. Points 1-6 represent the initial Metaward high-level view as presented by Robertson et al., (2024). This portion remains unchanged in this paper. **Points 7-9 introduce additional DFR measures to supplement the existing model.**

1. Tasks are meticulously generated and reviewed to ensure they conform to the specific requirements and regulations of the organization, thus fostering alignment with its overarching goals and standards.
2. Once tasks are approved, they are promptly assigned to employees along with clear deadlines and notifications. Additionally, periodic reminders are implemented, particularly catering to individuals who are motivated by loss aversion, to ensure task completion within stipulated timeframes.
3. In the event of task non-completion, employees face a cryptocurrency penalty deducted directly from their wallets, providing a tangible consequence for failure to meet obligations, and incentivizing timely completion.
4. Timely completion of tasks is incentivized through cryptocurrency rewards, which accrue and can be redeemed within specified timeframes. Employees are offered various redemption options, such as converting cryptocurrency to fiat currency or utilizing it for leisure time off, enhancing motivation and engagement.
5. Upon completion of tasks, employees are awarded icon-like badges, facilitating social comparison and recognition. These badges are designed with expiration dates to ensure ongoing relevance and up-to-date acknowledgment of accomplishments.
6. Employee rankings are subject to fluctuation based on their task completion status, appealing to individuals motivated by social comparison. These changes in rankings are regulated by expiration dates, maintaining a dynamic and competitive environment.
7. Detailed logs are maintained for each task, including information about the designated employee group and associated events such as task initiation, rewards, penalties, badge issuance, and ranking

adjustments. Validity checks are conducted on each logged event to ensure accuracy and alignment with organizational objectives.

8. Anomalies detected within the system trigger immediate alerts to designated personnel, with comprehensive details logged for analysis. In the event of an anomaly, the current Metaward session is terminated to safeguard against potential security threats or attacks.
9. All logged events and triggers are securely stored in an off-site database, ensuring data integrity and confidentiality. The utilization of the SecureRS system, as proposed by Singh et al., (2022), is recommended to enhance the robustness of the storage infrastructure and mitigate potential vulnerabilities.

The following section elaborates on the high-level conceptual model and breaks it down into separate component diagrams.

3.2 Digital Forensic Ready Metaward Model

In a previous study, Robertson et al., (2024) discuss existing Individual component diagrams for other processes within the Metaward model in detail. This is also summarized in section 2.3 of this paper. Figure 3 depicts the DFR component added to the Metaward Model, describing each step in the process below.

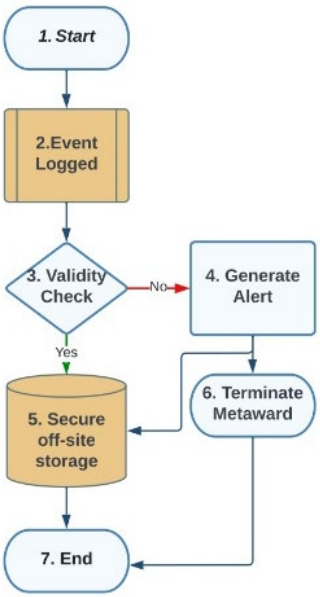

Figure 3: Digital Forensic Readiness Component Diagram

1. Start - Placeholder to begin the DFR component, at each point in the comprehensive model where an event is triggered.
2. Event logged – Each logged event contains specific information from the relevant event triggered, including a timestamp, user for the transaction and the action for the event, e.g. a penalty incurred, a reward added, rewards redeemed.
3. Validity Check – Each event logged is checked for validity. Should an anomaly be found, e.g. a reward for a task not allocated to the specific user, then the process continues to step 4, alternatively to step 5.
4. Generate alert – In the event of an anomaly occurring, an alert with the relevant details are generated and sent to the designated employee/s.
5. Secure off-site storage – The logged event is stored in a secure off-site database. The SecureRS system from (Singh et al., 2022) is recommended.
6. Terminate Metaward – Once the alert is triggered, the current Metaward session is terminated to prevent any further suspected attacks.
7. End – This placeholder marks the end of the DFR process, with the potential beginning of a digital forensic investigation as the process model is the starting point of any incident detection within the metaverse.

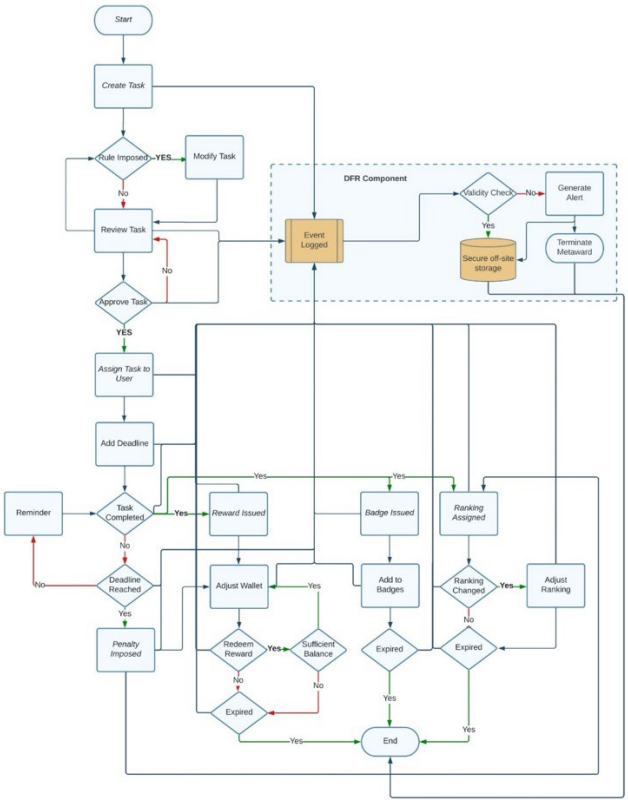

Figure 4: Metaward reward model (Robertson et al., 2024) with Digital Forensic Readiness

Figure 4 above, provides an overview of the comprehensive Metaward system, showcasing the incorporation of the Digital Forensic Readiness (DFR) component into the overall model. This integration marks a significant advancement in bolstering both security measures and employee motivation within the Metaverse. This ensures that events are logged at each critical point within the Metaward model, enabling Metaward to be a forensic-ready software system. The Metaward model caters to diverse employee motivations, incorporating badges for recognition-seeking individuals (Pombo et al., 2019; Pombo and Santos, 2023), leaderboards for those driven by social comparison (Christy and Fox, 2014; Dong and Zhu, 2023), rewards for incentive-driven employees , and timed penalties for those inclined towards loss aversion (Lin et al., 2023). Initially, rewards are offered in cryptocurrency, affording flexibility for subsequent redemption, which may include monetary benefits, instant rewards, or time off as per organizational preferences.

The following section delves into various case scenarios, to show the validity of implementing DFR into the Metaward model.

4. Case Scenarios

The following case scenarios are presented to illustrate the practical implications of integrating DFR into Metaward. These scenarios highlight how DFR can enhance security measures, detect fraudulent activities, ensure legal compliance, resolve disputes, and facilitate continuous improvement through feedback analysis. Each scenario demonstrates the value of DFR in safeguarding data integrity, promoting transparency, and maintaining the credibility of the reward system within organizational contexts.

Data Breach Investigation Efficiency: Suppose an organization using the Metaward Model experiences a data breach. With DFR integrated, the forensic readiness of their systems allows for swift and systematic investigation. Digital evidence such as access logs, transaction records, and user activity trails are readily available and properly preserved, expediting the identification of the breach's source, and minimizing its impact.

Fraudulent Activity Detection: Imagine an employee within the organization manipulating the Metaward model to fraudulently acquire rewards. DFR implementation enables real-time monitoring of system activities and behaviour analysis. Suspicious patterns, such as excessive reward claims or unusual access attempts, trigger alerts for investigation, preventing fraudulent behaviour and maintaining the integrity of the reward system.

Legal Compliance Assurance: Consider a scenario where the organization faces legal inquiries or litigation related to employee rewards and incentives. DFR ensures that all necessary digital evidence, such as reward distribution records, user consent acknowledgments, and system configurations, are systematically documented and securely stored. This ensures the organization's ability to comply with legal requests, demonstrate transparency, and protects against potential liabilities.

Employee Dispute Resolution: Suppose a dispute arises between employees regarding reward allocations within the Metaward model. DFR integration allows for comprehensive forensic analysis of relevant digital data, including logs, task completion records, and reward redemption histories. By providing objective and verifiable evidence, DFR facilitates fair dispute resolution, maintains employee trust, and upholds the credibility of the reward system.

Continuous Improvement through Feedback Analysis: In a scenario where employees provide feedback or suggestions for improving the Metaward Model, DFR enables systematic analysis of digital feedback data. By tracking user interactions, sentiment analysis, and feedback trends, organizations can identify areas for enhancement and prioritize feature development based on user needs and preferences. This iterative feedback loop ensures that the Metaward Model remains responsive to evolving organizational requirements and employee expectations.

The subsequent section highlights the scope and content of the research undertaken with this study.

5. Discussion

The integration of DFR into Metaward presents a significant advancement in enhancing both security measures and employee incentivization within the Metaverse. By incorporating DFR protocols, organizations gain robust mechanisms, to safeguard against potential security breaches, while leveraging virtual currencies to motivate and retain employees effectively.

The case scenarios illustrate the practical applications of DFR in various scenarios, showcasing its effectiveness in enhancing data breach investigation efficiency, detecting fraudulent activities, ensuring legal compliance, facilitating employee dispute resolution, and enabling continuous improvement through feedback analysis.

Through the implementation of validity checks, anomaly detection, and secure log storage, the enhanced Metaward model, provides law enforcement and justice systems, with timely and comprehensive digital evidence for investigations and litigation processes. Additionally, all logs are securely transmitted to an off-site database, with the recommendation to utilize the SecureRS model, presented by Singh et al., (2022) for preserving PDE while maintaining integrity. This further ensures the reliability and integrity of digital evidence storage.

Furthermore, the model aligns with readiness processes outlined in ISO/IEC 27043 (Valjarević et al., 2016), emphasizing its adherence to international security standards. By integrating event logging, secure log storage, and functionalities such as IP traceback/FIX protocol, as recommended by Kwon et al., (2019), Metaward ensures resilience and forensic preparedness, benefiting DF investigators and organizational security teams alike.

This research not only strengthens the security posture of organizations, but also enhances transparency, fairness, and trustworthiness in reward systems, ultimately benefiting end-users and promoting a safer and more secure digital environment.

In the subsequent section, this study summarizes its findings and presents potential avenues for future work.

6. Conclusion

The integration of DFR into the Metaward model marks a significant step towards enhancing both security measures and employee incentivization within the Metaverse. By incorporating DFR protocols, this study successfully strengthens the security infrastructure of Metaward while preserving its intrinsic benefits, particularly in utilizing virtual currencies to motivate and retain employees.

This research has achieved its primary objective of fortifying the Metaward model through the systematic integration of DFR. By ensuring the reliability and security of Metaward, organizations can confidently harness its capabilities to foster employee motivation and retention in virtual environments.

Several avenues for future research warrant exploration, including long-term assessments to fully comprehend the impact of DFR implementation on both employee engagement and organizational security posture. Additionally, further investigation into the scalability and adaptability of the Metaward model across different industries and cultural contexts would provide valuable insights into its broader applicability. Furthermore, continued refinement of the model, based on user feedback and the exploration of ethical considerations surrounding privacy and fairness, are essential for ensuring its effectiveness and ethical soundness in practice. This includes ongoing evaluations of privacy and fairness aspects to ensure the model's alignment with evolving ethical standards.

This study lays a solid foundation, for future research, aiming at the optimization of reward systems in the digital age, prioritizing security, and employee well-being in virtual work environments. Through collaborative efforts and ongoing refinement, the vision of a secure, incentivized, and ethically sound digital workplace can be realized.

References

Baror, S.O., Venter, H.S., 2013. Testing the harmonised digital forensic investigation process model-using an Android mobile phone, in: 2013 Information Security for South Africa. pp. 1–8.

Christy, K.R., Fox, J., 2014. Comput Educ 78, 66–77.

Daubner, L., Macak, M., Matulevičius, R., Buhnova, B., Maksović, S., Pitner, T., 2023. Addressing insider attacks via forensic-ready risk management, Journal of Information Security and Applications. Elsevier BV.

Dong, Y., Zhu, Q., 2023. How Downward Social Comparison Motivates Workers: A Structural Equation Model on Personality, Social Comparison Orientation, Motivation and Performance, in: ACM International Conference Proceeding Series. Association for Computing Machinery, pp. 207–212.

Farzan, R., Dimicco, J.M., Millen, D.R., Brownholtz, B., Geyer, W., Dugan, C., 2008. When the experiment is over: Deploying an incentive system to all the users.

Keshav, S., Cheriton, D.R., 2007. How to Read a Paper.

Kristyan, S.A., Suhardi, Juhana, T., 2020. Design Framework Forensics Readiness as a Service for Automatic Processing, ICITSI. ed. 2020 International Conference on Information Technology Systems and Innovation, Bandung - Padang, Indonesia.

Kwon, S., Jeong, J., Shon, T., 2019. Digital Forensic Readiness for Financial Network, PlatCon-19. ed. 2019 International Conference on Platform Technology and Service: proceedings, Jeju, Korea.

Lin, Y., Wang, J., Luo, Z., Li, S., Zhang, Y., Wünsche, B.C., 2023. Dragon Hunter: Loss Aversion for Increasing Physical Activity in AR Exergames. Association for Computing Machinery (ACM), pp. 212–221.

Muyambo, E., Baror, S.O., 2023. Digital Forensic Readiness Model for Internet Voting, in: European Conference on Cyber Warfare and Security. pp. 657–667.

Nugroho, H.A., Briliyant, O.C., Sunaringtyas, S.U., 2023. A Novel Digital Forensic Readiness (DFR) Framework for e-Government, in: Proceedings - 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity: Cryptography and Cybersecurity: Roles, Prospects, and Challenges, ICoCICs 2023. Institute of Electrical and Electronics Engineers Inc., pp. 184–189.

Ogunseyi, T.B., Adedayo, O.M., 2023. Cryptographic Techniques for Data Privacy in Digital Forensics IEEE Access.

Pasquale, L., Alrajeh, D., Peersman, C., Tun, T., Nuseibeh, B., Rashid, A., 2018. Towards forensic-ready software systems, in: Proceedings - International Conference on Software Engineering. IEEE Computer Society, pp. 9–12.

Pombo, N., Garcia, N., Alves, P., 2019. How to Get a Badge? Unlock Your Mind, IEEE Educon. ed. IEEE.

Pombo, N., Santos, H., 2023. Lessons Learned from the Development of a Computerised Badge-based Reward Tool for Student Engagement in Learning Activities, in: EDUNINE 2023 - 7th IEEE World Engineering Education Conference: Reimaging Engineering - Toward the Next Generation of Engineering Education, Merging Technologies in a Connected World, Proceedings. Institute of Electrical and Electronics Engineers Inc.

Rivera-Ortiz, F., Pasquale, L., 2019. Towards automated logging for forensic-ready software systems, in: Proceedings - 2019 IEEE 27th International Requirements Engineering Conference Workshops, REW 2019. Institute of Electrical and Electronics Engineers Inc., pp. 157–163.

Robertson, S., Baror, S.O., Venter, H.S., 2024. Metaverse: Virtual Currencies as a Mechanism for Employee Engagement and Retention ICCWS.

Roose, K., 2021. Why Did Facebook Become Meta? - The New York Times [WWW Document]. URL https://www.nytimes.com/2021/10/29/technology/meta-facebook-zuckerberg.html (accessed 10.2.23).

Singh, A., Ikuesan, R.A., Venter, H., 2022. IEEE Access 10, 19469–19480.

Valjarević, A., Venter, H., Petrović, R., 2016. ISO/IEC 27043:2015 — Role and application, in: 2016 24th Telecommunications Forum (TELFOR). pp. 1–4.

Valjarevic, A., Venter, H.S., 2012. Harmonised Digital Forensic Investigation Process Model. IEEE.

Watson, V., Bejiga, M., Bajramovic, E., Waedt, K., 2018. Designing Trustworthy Monitoring Systems Forensic Readiness for Safety and Security.

Xiao, N., Wang, Z., Sun, X., Miao, J., 2024. Alexandria Engineering Journal 86, 631–643.