Advancing Digital Forensics with the Integration of Cyber Threat Intelligence Technologies

Frank Junior Hoza Longfor
Florida A&M University
Tallahassee, FL, USA
Frankjunior1.hozalon@famu.ed

Yohn J. Parra Bautista
Florida A&M University
Tallahassee, FL, USA
yohn.parrabautista@famu.edu

Adi Chauhan
University of Florida
Gainesville, FL, USA
chauhanadi@ufl.edu

Hongmei Chi
Florida A&M University
Tallahassee, FL, USA
hongmei.chi@famu.edu

ABSTRACT

This research project explores a novel approach to bolstering digital forensics by integrating AlienVault, a leading security platform, with blockchain technology. By harnessing the capabilities of AlienVault for real-time threat detection and incident response and leveraging the immutable nature of blockchain for data integrity, this study proposes a framework for enhancing the reliability of digital forensic investigations. The tools used include AlienVault's Open-Source Security Information Management (OSSIM) platform for security information and event management (SIEM). Ethereum's blockchain-based ledger is used to log events detected by AlienVault OSSIM, ensuring each event log entry is time-stamped. Data sources for this study include a controlled setup network and the Open Threat Research (OTRF) Security Dataset of Windows event logs. These sources provide a comprehensive and realistic range of cyber-attack scenarios. By utilizing these datasets, the research evaluates how well the integrated system can detect and store threat information. The system's performance is assessed based on its accuracy in identifying attacks, the speed of its incident response, and the reliability of its forensic data. The expected result is a blockchain-enhanced forensic framework that mitigates common challenges in digital forensics, such as data tampering and chain of custody issues.

KEYWORDS

SIEM, Vulnerability analysis, blockchain, threat, risk, AlienVault, Cyber Threat Intelligence, Forensics Data.

ACM Reference Format:
Frank Junior Hoza Longfor, Yohn J. Parra Bautista, Adi Chauhan, and Hongmei Chi. 2026. Advancing Digital Forensics with the Integration of Cyber Threat Intelligence Technologies . In *2026 ACM Conference (ADMI 2026), March 26–29, 2026, 0rangeburg, SC, USA.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3696673.3723086

ADMI 2026, March 26–29, 2026, 0rangeburg, SC, USA

ACM ISBN 979-8-4007-1277-7/2026/04…$15.00
https://doi.org/10.1145/3696673.3723086

1 INTRODUCTION

In an age marked by the growing frequency and sophistication of cyber threats, digital forensics must address the pressing challenge of preserving the integrity and trustworthiness of forensic evidence [1]. As organizations increasingly depend on digital infrastructures, robust mechanisms for timely detection and effective response to cyber incidents have become indispensable. Consequently, there is a critical need for intelligent, real-time monitoring and mitigation systems capable of countering threats while ensuring the uncompromised preservation of forensic data [2].

In digital forensics investigations, there is a need for the secure collection and analysis of event data. A popular solution used by many cyber security analysts is security information and event management (SIEM) systems. However, the field faces many obstacles that can interfere with these investigations, including data tampering and the difficulty of maintaining a secure and verifiable chain of evidence [3]. These problems can undermine the credibility of forensic investigations and make it harder to effectively tackle cyber threats.

This research project introduces an innovative approach to these issues in log security by integrating AlienVault's Open-Source Security Information Management (OSSIM) system with blockchain technology. AlienVault OSSIM is a powerful open-source tool that offers most of the SIEM capabilities of its premium counterpart: AlienVault Unified Security Management (USM) [4]. OSSIM's functionalities include log analysis and correlation, threat monitoring, data visualizations, and security alert notifications. The only major difference is that OSSIM does not offer log management through AlienVault's USM Anywhere cloud service, which is another reason that OSSIM is suitable for this project.

Blockchain technology, exemplified by Ethereum's blockchain-based ledger, is a decentralized and tamper-proof method for logging and verifying data. Its use in digital forensics has shown promise to address issues related to data integrity but has not yet been used in conjunction with SIEM technology [5]. By ensuring that each log entry is time-stamped and immutable, this integration not only enhances the traceability and authenticity of forensic data but also simplifies the process of maintaining a secure chain of events.

To evaluate this approach, the study utilizes data from two key sources: a controlled setup network and the Open Threat Research (OTRF) Security Dataset of Windows event logs.

- The controlled network environment offers a limited range of security events to evaluate the system's performance in an environment more indicative of the average computer setup [3].
- The OTRF Security Dataset [6] is a comprehensive collection of Windows event logs, simulating various cyber-attack scenarios. It includes logs mapped to the MITRE ATT&CK® Matrix [7], a knowledge base of adversarial tactics and techniques. Since these logs were mapped to an industry standard for attack identification, they allow for more thorough testing of the SIEM blockchain system.

This paper is organized as follows: The related works found from our literature search are presented in Section 2. In Section 3, we discuss the details of our chosen datasets, environmental setup, and the tools used. The research methodology is outlined in Section 4. Our preliminary results are contained in Section 5, where we share the framework found and further discussion on the paper's limitations. Finally, Section 6 features our conclusions and how we plan to further our research.

2 RELATED WORK

This research draws upon several key studies that explore the early stages of development for the intersection of blockchain technology and digital forensics. Up until now, little work has been done within the context of enhancing SIEM systems with blockchain ledgering; hence, there is a need to assess similar studies to expand upon this research.

2.1 BlockSIEM: Blockchain-enhanced SIEM

The BlockSIEM framework from [3] proposes a hybrid architecture combining SIEM capabilities with blockchain technology to enhance the security and reliability of event monitoring systems. Their model integrates blockchain's immutability and transparency features to store and verify security events, thus ensuring that logs are immutable and auditable. This integration allows organizations to detect and respond to security incidents more efficiently. Additionally, BlockSIEM supports decentralized logging and auditing, providing a distributed solution that mitigates the risks associated with centralized log management systems, such as single points of failure and susceptibility to insider threats.

2.2 Cybersecurity through Blockchain

Zangana [8] and Mathew [5] provides a review of the increased applications of blockchain and AI in cybersecurity. The paper examines various use cases, such as using blockchain to bolster the security of the Internet of Things, networks, and data. Many researchers has been reviewed, but research has yet to be done on merging blockchain technology with SIEM, such as AlienVault OSSIM. This paper highlights the inherent immutability of blockchain, which ensures data integrity and security. The study emphasizes that any attempt to modify a block would compromise the entire blockchain, making it an ideal solution for applications requiring robust security measures, such as SIEM technologies.

2.3 Designing blockchain-based SIEM 3.0 system

Similar to [3], the work of [9] offers a comprehensive framework for integrating blockchain with SIEM. The paper provides specific examples of security events that could trigger the creation of new blocks within the blockchain, demonstrating the practical implementation of this integration. This approach aligns closely with our study, making it a valuable point of reference when designing our procedures and methodology.

2.4 Using AI to Combat Cyber Threat

We explore how AI technologies, integrated into OSSIM, improve threat detection, incident response, and overall security posture from past research papers. Key aspects of the research might include case studies or experiments demonstrating the effectiveness of AI-enhanced OSSIM in mitigating various types of cyber threats, such as malware, phishing attacks, or insider threats.

Further insights are provided by [10], which discusses the utilization of the Open Cyber Threat Intelligence platform for accessing a rich database of malware-related data. This paper also outlines the capabilities of AlienVault in providing pulses related to different types of malware. These concepts are directly relevant to our research, which leverages AlienVault's OSSIM for real-time threat detection and incident response.

A comparative analysis of the security features and performance of various open-source SIEM solutions, including AlienVault OSSIM, is conducted. This study [4] reinforces the suitability of OSSIM as a reliable tool for security information and event management, supporting our choice of using OSSIM in our proposed framework.

The OTRF dataset of event logs is applied to develop a machine learning detection model, SeckG [6]. Previously known in this paper as Mordor, but since its change, this paper's use of the OTRF dataset provides a precedent for using these event logs in threat detection and analysis.

2.5 Research Gaps and Proposed Approach

Despite significant advancements in digital forensics and cybersecurity, notable gaps remain in the integration of blockchain technology for secure data protection and forensic evidence management. Existing studies have explored the application of blockchain within cybersecurity ecosystems and its potential integration with Security Information and Event Management (SIEM) technologies. However, most of this work remains conceptual or theoretical, with limited implementation of practical and deployable solutions that demonstrate how blockchain can be effectively incorporated into real-world forensic and threat-intelligence infrastructures[10, 11], Among the available SIEM platforms, AlienVault OSSIM is widely recognized as one of the most capable open-source solutions, offering strong performance in threat detection, event correlation, and security monitoring [12]. Despite its capabilities, there is currently little research addressing how blockchain can be systematically integrated with OSSIM to enhance the integrity, traceability, and reliability of forensic data [13].

To address this gap, this paper proposes a framework that integrates blockchain technology with AlienVault OSSIM [4] to support secure cyber threat intelligence and digital forensic processes. The

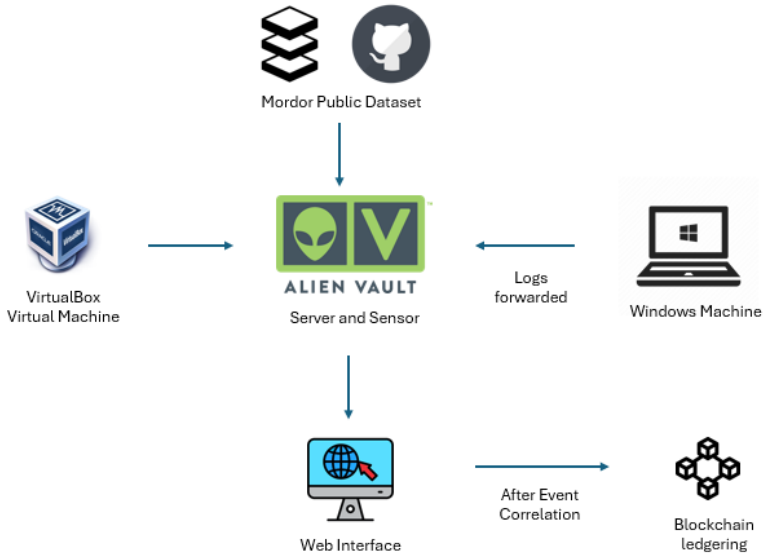

Fig. 1: Environment Setup

proposed approach aims to provide a practical and implementable solution that strengthens evidence integrity, improves data immutability, and enhances the trustworthiness of forensic artifacts within SIEM-driven security environments.

3 CASE STUDY

In this case study, we employ a combination of tools, datasets, and a simulated network environment to evaluate the effectiveness of the integrated SIEM system. An important element of this test environment was to ensure we used both benign and malicious data to keep our research as true as possible to what real-world SIEM systems deal with.

- AlienVault OSSIM [10]: This open-source SIEM platform will be used for security information and event management. It is central to collecting, analyzing, and managing security event logs in real time.
- Ethereum Blockchain [14]: Ethereum's blockchain-based ledger will ensure the immutability and integrity of the log entries by time-stamping and storing them decentralized.
- VirtualBox: This virtualization tool will be used to set up and manage the virtual machines needed for the testing environment.

3.1 Dataset

Controlled Setup Network: A simulated network environment will be created to generate various security events and attack scenarios for testing purposes.

OTRF Dataset (https://github.com/OTRF/Security-Datasets): A comprehensive collection of Windows event logs that simulate various cyber-attack scenarios. This dataset provides a realistic testing ground for evaluating the detection and response capabilities of the integrated system. It is primarily composed of events related to attacks as well as the set of friendly events that were also occurring at the same time as the attack. There are both network capture data and event data, but only the event logs were used for this research. The event data is stored in JSON files and is easily ingested by the OSSIM SIEM. A sample log is taken from a file of a credential access event to show the structure of a typical log entry in the data set:

"SourceName":"Microsoft-Windows-PowerShell",
"ProviderGuid":"a0c1853b-5c40-4b1587663cf1c58f985a",
"Level":"5","Keywords":"0x0",
"Channel":"Microsoft-Windows-PowerShell/Operational",
"Hostname":"DC01.pandalab.com", "TimeCreated":"2023-07-19T09:05:56.029Z",
"@timestamp":"2023-07-19T09:05:56.029Z", "EventID":4105,
"Message":"Started invocation of ScriptBlock

3.2 Scenario

The study will utilize both the controlled network environment and the OTRF dataset to create realistic scenarios. These scenarios will include a variety of cyber-attack patterns to evaluate the system's performance thoroughly. The data set contains attacks such as credential access, defense evasion, privilege escalation, etc. Other than malicious event data, OTRF also has benign data. This makes it so there is more comprehensive coverage for all types of logs in our testing.

Components of the data set:

- Windows Event Logs: Logs generated by Windows operating systems, including security, application, and system logs in JSON format.
- Attack Simulations: Scenarios replicating common and advanced attack techniques used by adversaries.
- Metadata: Additional information about the logs, such as timestamps, event IDs, and descriptions of the events.

3.3 Setting Up Testing Environment

In Fig. 1, the testing environment is shown. The first step involves creating a controlled testing environment to deploy and test the integrated system. This is achieved using VirtualBox to set up virtual machines (VMs) for the AlienVault server and sensors. The testing environment includes:

AlienVault Server VM: This VM is configured with the AlienVault OSSIM platform to serve as the central SIEM system for security information and event management. **Specifications:** 8192 MB allotted memory, three processors, Bridged Network Adaptor.

AlienVault Sensor VM: This VM acts as a sensor to collect logs from various sources within the network and forward them to the AlienVault server for analysis. **Specifications:** 6144 MB allotted memory, two processors, Bridged Network Adaptor.

Windows Machine: A Windows Machine is set up to generate event logs that mimic real-world scenarios and cyber-attack activities. **Specifications:** Microsoft Windows 11 Lenovo Thinkpad T14 AMD Ryzen 7 pro 16GB.

3.4 Approach

In order to categorize the event logs, the first step is to employ the AlienVault sensor to gather the data from our host machine. As depicted in Fig. 2, after the logs are created in the testing environment and the OTRF files are integrated into the system, the data is forwarded to the AlienVault sensor/server. We rely on OSSIMS machine learning algorithms in combination with its threat intelligence to detect abnormal or malicious data. These abnormalities are learned patterns that the intrusion detection system can predict, which we use to group the events.

4 METHODOLOGY

Because of our chosen testing environment, it is necessary for our methodology to operate on the same network. Log generation, forwarding, and processing occur on the same system and must function smoothly. The Windows machine provides event logs, forwarded to the AlienVault OSSIM for processing. The logs are generated using Sysmon and forwarded with NXLog, then analyzed with the MITRE ATT&CK® Matrix to detect malicious activities. To ensure data integrity, critical log entries are time-stamped and recorded on the Ethereum blockchain.

4.1 Design

The AlienVault Sensor, Server, and Windows machine all operate under the same network, allowing for seamless data transfer between the three. The Windows Event Logs are generated by the computer and forwarded to Alienvault OSSIM in Syslog format. The Sensor, acting as an aggregator, processes and normalizes these different data inputs before sending them to the OSSIM server. Because of this, OSSIM is able to read many different formats, such as JSON, syslog, and EVT. The SIEM system then combines all the data into one digestible format for further analysis.

4.2 Data Collection

In this step, logs are aggregated from our machine and the OTRF data sources using the AlienVault Sensor integrated into the SIEM system. Specifically:

Windows Event Log Generation: This project relies on the System Monitor (Sysmon) log-generating agent for our in-machine event logging. [15]. We left OSSIM active for four hours over several intervals while the machine performed regular tasks like settings changes, Microsoft Office Suite, Google Chrome, etc. These normal usage logs made up the first part of our OSSIM data. During this time, Sysmon monitored the activity and generated logs to the Windows System Event Log. These logs contain detailed information about network connections and process creations and even detect changes to a file's timestamp. These things can be modified and affected by Malware and other anomalous activity, which Sysmon can report in the logs. We have configured Sysmon to create logs in Syslog format. Syslog is a standard protocol for system logging [16]. It contains the following components: Header that includes version, timestamp, hostname, application, process ID, message ID, application, and priority. Structured data in a key=value order. A message describing the event and severity value from 0-7, with 0 indicating an emergency message and 7 being the least threatening. An example of one such log can be found in Section III.

Windows Event Logs Forwarding: Logs from the Windows Event Viewer are forwarded to the AlienVault Sensor using NXLog in Syslog format. Nxlog is a multi-platform log management tool that supports the collection and forwarding of log data in various formats [17]. We configured NXLog with the Syslog standard User Datagram Protocol (UDP) on port 514 to ensure information transfer.

OTRF Event Log Forwarding: For the second part of our OSSIM data, we made use of the publicly available OTRF Security Event dataset. Since these are historical files, there was no need for log generation. The OTRF data set was configured to be ingested by OSSIM using Nxlog file forwarding over the om_tcp protocol. This module initiates a TCP connection to the sensor and transfers the log data. NXLog can readily accept historical log files from the OTRF dataset, as they are already in JSON format. This also makes it easier for OSSIM to receive the logs in one of the formats that it is made to collect.

4.3 Abnormal Detection from Log data

Once the logs are collected, they are processed and analyzed using the MITRE ATT&CK® Matrix, which is integrated into the AlienVault system, as seen in Fig. 3 below. This integration allows OSSIM to detect malicious activities and uses identification numbers to classify different attacks, helping the system to distinguish between regular traffic and potential intrusions. One such example of an abnormal detection is the malware identification in Table 1. OSSIM uses its pattern recognition functionalities to alert the user of malware infection from the system modification and script execution activity within the log file.

4.4 Blockchain Integration

To ensure the integrity and immutability of critical log entries, a blockchain-based ledger will be utilized. Ethereum's blockchain technology is employed to record these log entries. Each critical log entry will be time-stamped and added to the blockchain, creating an immutable record of events. The use of blockchain guarantees that once an entry is recorded, it cannot be altered or tampered with,

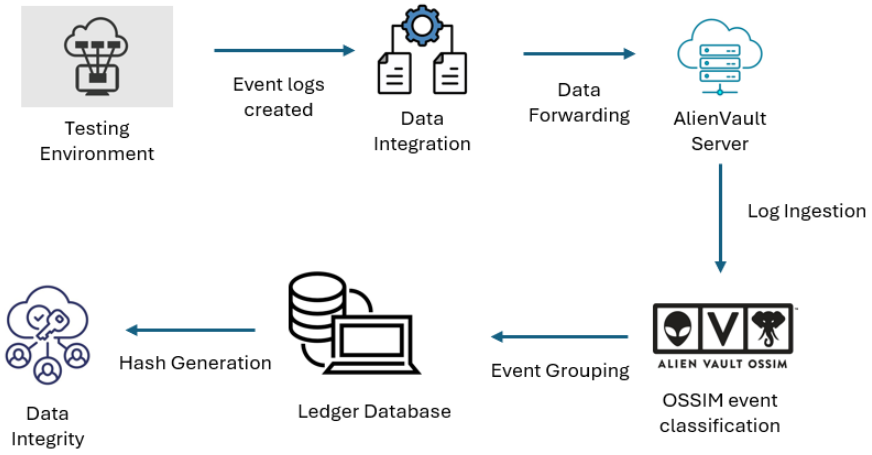

Fig. 2: Proposed Approach

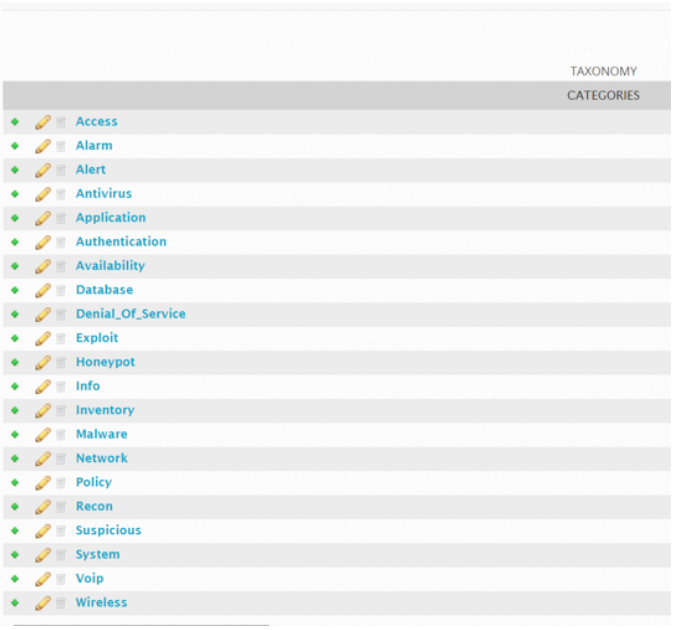

Fig. 3: Attack Categories

thus maintaining the provenance and integrity of the forensic data. This step is crucial for preventing data tampering and maintaining the chain of custody.

4.5 Smart Contract Deployment and Chain Verification

For this paper, we developed and deployed a smart contract called `ForensicLogger` on Ethereum Sepolia testnet (chain ID 11155111) at address: `0x2A48Cb0696fEcfEC80DDb33Ee708D5F981c4dd4F` (deployment transaction `0x5693...824f`, block 10451210).

The source code was independently verified via Sourcify, confirming an exact match of both the runtime and creation bytecode against the published Solidity source. This verification ensures that the contract executing on-chain is identical to the code described in Section 4.4, satisfying a key requirement for reproducible and auditable forensic tooling.

This function was called on the live contract via Remix IDE, using the deployer wallet `0x39b4...09C5A`. The decoded output was:

```
decoded output {
    "0": "bool: chainIntact  true",
    "1": "uint256: brokenAt  0"
}
```

The return value `chainIntact = true` confirms that every `prevHash` pointer in the on-chain ledger correctly references the hash of its preceding entry, with no breaks or inconsistencies detected across the full chain. The value `brokenAt = 0` is only meaningful when `chainIntact` is `false`; its presence here simply indicates that no tampered entry was found at any position. Together, these results provide direct, on-chain cryptographic evidence that the forensic log has not been altered since the time of submission satisfying the chain-of-custody integrity requirement central to this research. Table 1 summarises the deployment and verification metrics recorded during testing.

Table 1: ForensicLogger Deployment and Verification Metrics (Sepolia Testnet)

Metric	Value
Network	Ethereum Sepolia (chain ID 11155111)
Contract Address	`0x2A48...4d4F`
Deployment Transaction	`0x5693...824f`
Block Number	10,451,210
Transaction Index	10
Compiler	solc 0.8.31+commit.fd3a2265
Bytecode Verification	Exact Match (Sourcify)
`verifyChain()` result	`chainIntact = true`
`brokenAt`	0 (no tampering detected)

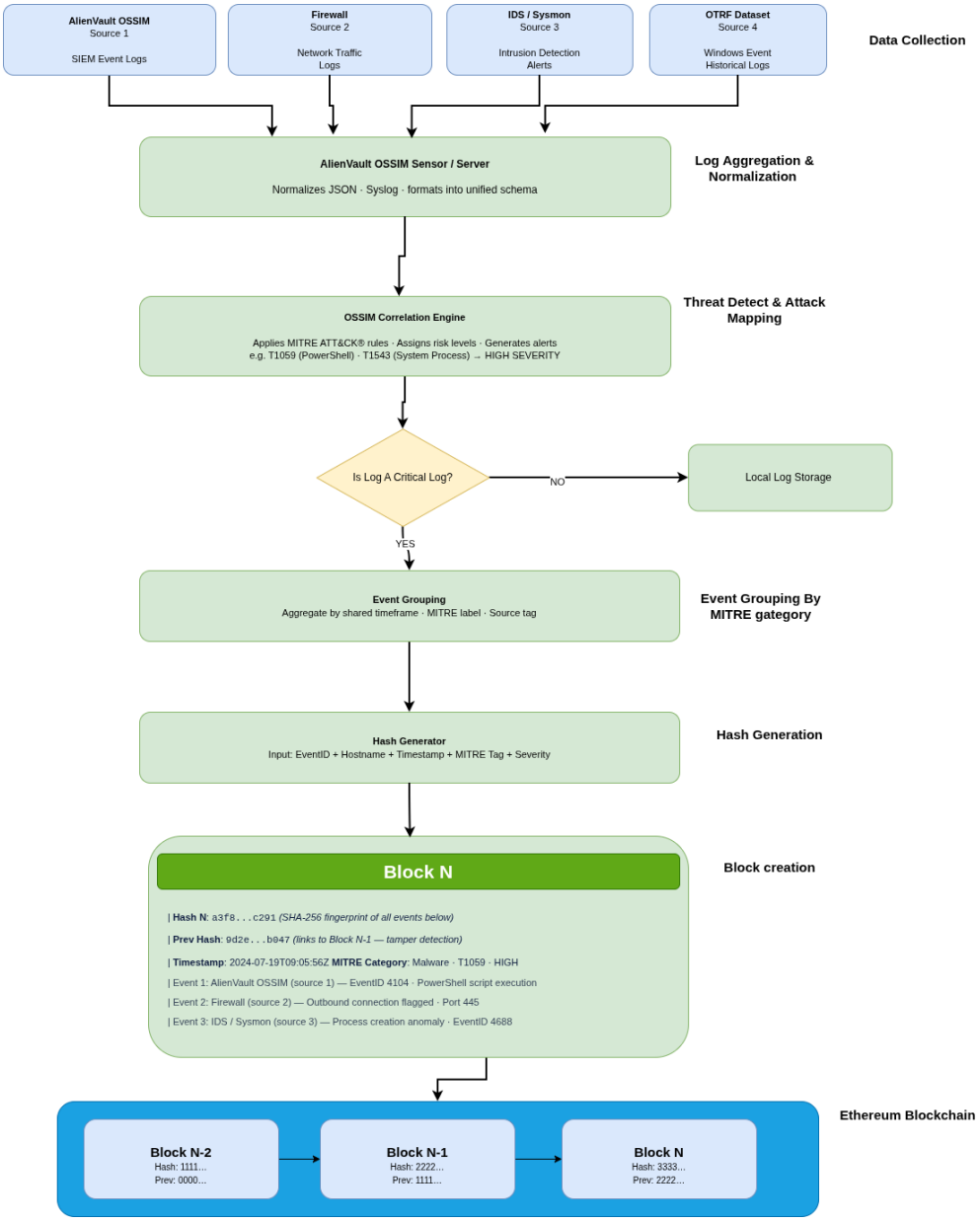

Fig. 4: Block Creation Workflow: from multi-source event collection through OSSIM normalization, MITREATT&CK® detection, SHA-256 hashing, and immutable Ethereum ledger storage.

5 PRELIMINARY RESULTS

After the data was received by OSSIM, the SIEM system successfully applied correlation rules to identify the risk level of every event. OSSIM normalizes differently formatted log entries into a single configuration to allow its correlation engine to detect behavior patterns. This allowed for further grouping of logs alongside their event IDs. Moving forward, this grouping is essential for blockchain creation. The blocks should be organized by event groups so that they can be more easily accessed by the security team. One such grouping method is to utilize the categories given by OSSIM in Fig. 3. It contains anomalous event listings, such as malware, recon, exploits, benign system info, antivirus, etc. Each block would be labeled with such classifiers, along with the IDs for the events that constitute the log information.

To demonstrate how OSSIM groups events together to paint a full picture of possible attacks on a system, an example of a malware infection is provided in Table 1. Event log files from the OTRF database are used here. In addition to the event IDs and MITRE mapping, OSSIM also generated an alert level of High Severity for a potential malware infection. This structured grouping of security events is pivotal in consolidating threat detection data onto a blockchain.

Through the literature review and testing of the OSSIM tool with a diverse range of data, a block creation workflow has been created, as depicted

Table 2: OSSIM Threat Detection

Description	Detection of Malware Infections
Event IDs	4104, 4688, 7045
MITRE ATT&CK Mapping	T1059: Command and Scripting Interpreter
	T1059.001: PowerShell
	T1543: Create or Modify System Process
Alert	High Severity

in Fig. 4 above. Security events are detected and logged by various systems within the network infrastructure, each tagged with its source for traceability. These events are aggregated based on specific timeframes or shared characteristics (such as MITRE ATT&CK labels), allowing for efficient data management.

Once grouped, a unique hash is generated for each set of correlated events using the SHA-256 cryptographic algorithm, producing a fixed-length 256-bit digest that serves as a tamper-evident digital fingerprint of the event group.The hash input is constructed by concatenating six fields drawn directly from the OSSIM event record and the MITRE ATT&CK® classification assigned by the correlation engine:

$$H = \textit{SHA-256}(\textit{EventIDs} \parallel \textit{Hostname} \parallel \textit{MITRETag} \parallel \textit{MITRECategory} \parallel \textit{Severity} \parallel \textit{Timestamp}) \quad (1)$$

Through this approach of tagging, grouping, hashing, and block creation, organizations can ensure the reliability and accuracy of their security event logging when used in combination with AlienVault OSSIM or other SIEM systems.

5.1 Comparison

There are some studies that have found similar results for the criteria of creating a new block with security information. Botello et. al [3] details a block comprising multiple events that correlated to a single situation. Similarly, we have identified a way of classifying events to input them onto a block using AlienVault OSSIM as shown in Fig. 4. The order of the chain and automatic deletion of blocks is discussed within [18]. Both their work and ours suggest chronological order for block creation, but we have yet to implement automatic block creation and deletion.

5.2 Limitations and Discussion

Due to the limitations of Ethereum's blockchain, it would be too costly to store every event on the chain. Our research has yet to address these issues, but there are some potential solutions for reducing file sizes and costs. In the future, we could use the Interplanetary File System (IPFS). IPFS is a distributed file system that allows data to be stored off-chain but accessed globally, so more security data can be stored without failure [19, 20]. Each file is given a unique hash, which can be pushed to the blockchain rather than the entire security event. In addition, many other datasets are available for event logs in different formats [21, 22]. These can be used to further assess the reliability of the SIEM blockchain system with diverse inputs [23].

6 CONCLUSION

This research has presented a novel approach to secure log storage by integrating AlienVault OSSIM with Ethereum's blockchain technology. We have established a robust framework that significantly improves the reliability of forensic data. Our results indicate that the integrated system accurately detects and logs security events. The system performed well in identifying attacks and responding to incidents promptly, meeting the high standards for practical digital forensics tools.

However, there is still work to ensure full functionality with blockchain creation. Future work would involve using smart contracts to automate block creation from OSSIM event data [11]. This can be achieved by using the simple programming language for blockchain, such as MOVE [24] or GO [25]. Kali Linux may also be useful for creating in-house attack data with a plethora of tools for penetration testing and ethical hacking. There are many applications, such as database assessment, password attacks, and various other exploitation tools [26]. To enhance security monitoring, additional network devices such as firewalls, routers, and switches can also be integrated into the same network.

The integration of Cyber Threat Intelligence (CTI) with digital forensics represents a pivotal step toward enhancing the effectiveness and intelligence of modern cyber investigations, particularly in light of the rapid advancement of Large Language Models (LLMs) [27]. While this work demonstrates the feasibility and practical benefits of incorporating CTI-driven insights into forensic workflows, it also highlights several open research challenges [28]. Future research should move beyond preliminary proof-of-concept implementations and focus on the development of scalable, trustworthy, and legally defensible AI-augmented forensic frameworks [29]. Such efforts will be critical to enabling adaptive, intelligence-driven forensic ecosystems capable of supporting investigators in addressing the scale, complexity, and evolving sophistication of contemporary cyber threats.

ACKNOWLEDGMENT

This project was supported in part by Title III funding received from the US Department of Education to Florida A&M University. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the US Department of Education or Florida A&M University.

REFERENCES

[1] P. Alaeifar, S. Pal, Z. Jadidi, M. Hussain, and E. Foo, "Current approaches and future directions for cyber threat intelligence sharing: A survey," *Journal of Information Security and Applications*, vol. 83, p. 103786, 2024.
[2] D. R. Arikkat, P. Vinod, R. R. KA, S. Nicolazzo, A. Nocera, G. Timpau, and M. Conti, "Ostis: A novel organization-specific threat intelligence system," *Computers & Security*, vol. 145, p. 103990, 2024.
[3] J. V. Botello, A. P. Mesa, F. A. Rodríguez, D. Díaz-López, P. Nespoli, and F. G. Mármol, "Blocksiem: Protecting smart city services through a blockchain-based and distributed siem," *Sensors*, vol. 20, no. 16, p. 4636, 2020.
[4] J. Manzoor, A. Waleed, A. F. Jamali, and A. Masood, "Cybersecurity on a budget: Evaluating security and performance of open-source siem solutions for smes," *Plos one*, vol. 19, no. 3, p. e0301183, 2024.
[5] A. R. Mathew, "Cyber security through blockchain technology," *Int. J. Eng. Adv. Technol*, vol. 9, no. 1, pp. 3821–3824, 2019.
[6] S. Kriaa and Y. Chaabane, "Seckg: Leveraging attack detection and prediction using knowledge graphs," in *2021 12th International Conference on Information and Communication Systems (ICICS)*, pp. 112–119, IEEE, 2021.
[7] S. Roy, E. Panaousis, C. Noakes, A. Laszka, S. Panda, and G. Loukas, "Sok: The mitre att&ck framework in research and practice," 2023.
[8] H. Zangana, "Blockchain technology in ai-driven cybersecurity: Strengthening trust in financial and digital security systems," *Jurnal Ilmiah Computer Science*, vol. 4, no. 1, pp. 49–49, 2025.
[9] N. Miloslavskaya, "Designing blockchain-based siem 3.0 system," *Information and Computer Security*, vol. 26, pp. 491–512, 09 2018.
[10] M. Miranda, A. Talarico, B. L. Sena, G. Paternezzi, R. Bottura, V. Bastos, and D. Sanches, "Outsmating malware: Using ai to combat wannacry," *Revue Africaine de Recherche en Informatique et Mathématiques Appliquées*, 2024.
[11] J. C. López-Pimentel, L. A. Morales-Rosales, and R. Monroy, "Rootlogchain: Registering log-events in a blockchain for audit issues from the creation of the root," *Sensors*, vol. 21, no. 22, p. 7669, 2021.
[12] S. Chakraborty, "Next-gen digital forensics: Investigating cybercrime in the era of ai, blockchain, and the dark web," *The Science of Criminal Investigations*, p. 286, 2026.
[13] D. Hariyani, P. Hariyani, S. Mishra, and M. K. Sharma, "A literature review on transformative impacts of blockchain technology on manufacturing management and industrial engineering practices," *Green Technologies and Sustainability*, vol. 3, no. 3, p. 100169, 2025.

[14] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[15] V. Mavroeidis and A. Jøsang, "Data-driven threat hunting using sysmon," in *Proceedings of the 2nd international conference on cryptography, security and privacy*, pp. 82–88, 2018.

[16] P. Sahoo, R. Chottray, G. Jena, and S. Pattnaiak, "Syslog a promising solution to log management.," *International Journal of Advanced Research in Computer Science*, vol. 3, no. 3, 2012.

[17] R. Vaarandi and P. Niziński, "Comparative analysis of open-source log management solutions for security monitoring and network forensics," in *Proceedings of the 2013 European conference on information warfare and security*, pp. 278–287, 2013.

[18] M. Koutenskỳ and V. Veselỳ, "Oracleboros: Reusing hyperledger fabric mechanisms to provide oracle functionality," in *2025 7th International Conference on Blockchain Computing and Applications (BCCA)*, pp. 139–144, IEEE, 2025.

[19] C. Maraveas, M. Rajarajan, K. G. Arvanitis, and A. Vatsanidou, "Cybersecurity threats and mitigation measures in agriculture 4.0 and 5.0," *Smart Agricultural Technology*, vol. 9, p. 100616, 2024.

[20] M. Naz, F. A. Al-zahrani, R. Khalid, N. Javaid, A. M. Qamar, M. K. Afzal, and M. Shafiq, "A secure data sharing platform using blockchain and interplanetary file system," *Sustainability*, vol. 11, no. 24, p. 7054, 2019.

[21] M. Allegretta, G. Siracusano, R. Gonzalez, and M. Gramaglia, "Are crowd-sourced cti datasets ready for supporting anti-cybercrime intelligence?," *Computer Networks*, vol. 234, p. 109920, 2023.

[22] Y. Keim and A. Mohapatra, "Cyber threat intelligence framework using advanced malware forensics," *International Journal of Information Technology*, vol. 14, no. 1, pp. 521–530, 2022.

[23] M. Beckmeyer and A. Phadke, "Blockchain-enhanced siem for defense networks," *Blockchain and Cryptocurrency*, p. 17, 2025.

[24] A. Welc and S. Blackshear, "Sui move: Modern blockchain programming with objects," in *Companion Proceedings of the 2023 ACM SIGPLAN International Conference on Systems, Programming, Languages, and Applications: Software for Humanity*, pp. 53–55, 2023.

[25] L. Olivieri and L. Negrini, "Don't panic: Error handling patterns in go smart contracts and blockchain software," in *2025 7th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pp. 1–9, IEEE, 2025.

[26] M. S. Rich and M. P. Aiken, "An interdisciplinary approach to enhancing cyber threat prediction utilizing forensic cyberpsychology and digital forensics," *Forensic Sciences*, vol. 4, no. 1, pp. 110–151, 2024.

[27] Y. Meng, L. Tang, F. Yu, J. Jia, G. Yan, P. Yang, and Z. Xi, "Uncovering vulnerabilities of llm-assisted cyber threat intelligence," *arXiv preprint arXiv:2509.23573*, 2025.

[28] P. Balasubramanian, S. Liyana, H. Sankaran, S. Sivaramakrishnan, S. Pusuluri, S. Pirttikangas, and E. Peltonen, "Generative ai for cyber threat intelligence: applications, challenges, and analysis of real-world case studies," *Artificial Intelligence Review*, vol. 58, no. 11, p. 336, 2025.

[29] B. I. Onyeashie, M. Abubakar, P. Leimich, S. McKeown, and G. Russell, "Privacy-preserving and scalable digital evidence management: A hyperledger fabric architecture with growth projections for law enforcement," in *2025 International Conference on New Trends in Computing Sciences (ICTCS)*, pp. 105–112, IEEE, 2025.