IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

Real-Time Security Context Awareness in Multifactor Authentication using Wazuh SIEM

Manoj P[1] and Prashant Ankalkoti[2]
Postgraduate Student, Department of Master of Computer Applications[1]
Assistant Professor, Department of Master Computer Applications[2]
Jawaharlal Nehru New College of Engineering, Karnataka, India

Abstract: *In the current cybersecurity environment 16 billion of the customer passwords of various platforms were leaked, and therefore the traditional methods of authorization, which are passwords, can no longer be considered reliable. In this study, a new integration of Multifactor Authentication (MFA) is proposed to integrated with Wazuh SIEM to provide a context-aware authentication that is responsive to the dynamic threat environment. This system leverages the time based security that MFA with PyOTP offers but with the benefit of jury based detection in the form of log analytics and anomaly detection that Wazuh offers. The system also skyrockets access control, sends notifications in real-time and has forensics capability through interactive dashboards. This architecture has shown to provide a significant boost to resilience in the areas of brute-force attacks, phishing, session hijacking and unauthorized access, according to our findings.*

Keywords: Multifactor Authentication (MFA)**,** Wazuh SIEM **,** PyOTP and JWT

I. INTRODUCTION

In the present digitized world of heightened connectivity, the threats of data security to personal and commercial information are becoming more sophisticated and un wearying. Cyberattacks such as phishing, credential stuffing, brute-force logins have ceased to be a phenomenon that can be observed once a day. Alas, in many organizations, to this day, an old-fashioned kind of authentication is used, such as the use of usernames and passwords which are weak against present day attack vectors. This increasing susceptibility requires something more than increased user verification measures; it requires a capacity to interpret where access attempts are taking place in the context of what happens with those access attempts.This project will seek to overcome these problems by developing a context-aware MFA solution with real-time analysis of security logs in use with the Wazuh SIEM. The aim is to transition to dynamic verification where the security context of every access attempt is pro-actively monitored, analyzed and responds.

At the core of this system is MFA: the generation of the time-sensitive OTPs with PyOTP and of secure communication sessions with JSON Web Tokens (JWT). All these mechanisms will be the ones that allow maintaining physical access to information, despite the verification mechanism, such as the password, being compromised, since there will be a mechanism of verification that is related to time. Nevertheless, this project goes even further -- it also has an agent in the form of Wazuh that allows behavioral awareness. Real time recording and tracking is also provided for each authentication. Events like repeated logins, failed logins, logins at geolocations never used before, logins that occur during the time a known attack was detected, are reported within a few seconds. The Wazuh administrators will see the events occurring and in the event of a requirement, execute automated actions that include invalidating the sessions and blocking the IP address.

Its logic deriving can be related to the practical necessity to provide cyber-defensical-based applications in the real world. The dynamic security controls are however required due to increased targeting and evasion capability of attacks. MFA and SIEM are synergistic and complement each other with each defining end-goals that complement one another. The integration of such systems with each other is a proactive front-toothed approach as opposed to reactive and check who you are the authentication does today. The synergies are expected to build a scalable, modular and affordable

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

security architecture that can be built to serve the adaption of any enterprise, academic or even an individual security requirement.

In a nutshell, this determines a more resilient method of access control - more brilliant than targeted attacks based on global authentication - situational awareness that could be disintegrated due to the prevailing cyber threats

II. LITERATURE SURVEY

Rakesh Bhavsar ,Vishvjit Thakar [1] resarch presents the concept of a low-cost, open-source architecture of the Operations Center for Security (OCS) that can be used to improve cybersecurity threats detection and response within organizations. It integrates the Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) capabilities by leveraging Wazuh to monitor, the Suricata to detect the intrusions in the network, and The Hive to manage the incidents as a case. The system was also tested by simulating cyberattacks of malware downloads, brute force attacks and DoS attacks. Results validated the premise of the setup in identifying threats, evaluating exposures and resolving incident responses. On the whole, the study demonstrates that the organizations can achieve a high level of the security visibility and response management with cost-efficient and open-source OCS framework.

Deepanshu Garg, Honey Paptan [5] research has shown that the use of Multi-Factor Authentication (MFA) has been established as a must-have tool against cyber threats in an increasingly connected world. It is centered around the concept and evolution of an MFA regime that includes authentication in the form of extended authentication (fingerprints or facial recognition), One-Time Passwords (OTPs) and hardware tokens such as USB security key. By merging such approaches into one system, the paper will explain how Python can be used to devise a secure and interactive authentication mechanism that not only can make the protection of access and risk of losing access to a third party minimal.

Dario S Czech, Zlatan Moric [3] compares two of the leading SIEM systems - IBM QRadar (commercial vendor) and Wazuh (open source) - by comparing their features, configuration and implementation. The tools are evaluated in the way they react to and find real life security attacks that are frequent in organizations. Relying on the practical testing and analyzing the real life scenario of each SIEM system, the study identifies the advantages and limitations of each one of these SIEM systems. These findings present a notion of the efficacy, responsiveness, and adequate adaptation of the QRadar and Wazuh in terms of enterprise IT infrastructure security.

Diogo Donadoni Santos [4] specialises in the improvement of eHealth cybersecurity preparedness and response. It will seek to establish a specific system, which is capable of detecting cyber-attacks on critical healthcare assets and estimate their impact and take automated cyber-defenses to make the operations resilient. The system will have a positive effect on incident response in eHealth organizations since it would enable responding to breaches in a timely manner and building organizational resilience with time. Of significance to the work is that it opened with the idea that cybersecurity risks in healthcare environments need a proactive and structural response to take care of them.

Conor Gilsenan [6] argues the security and usability concerns surrounding Time-based One-Time Password (TOTP) algorithms under two-factor authentication (2FA), and is particularly concerned with Backup and recovery. In an experiment, researchers reverse engineered 22 of the most popular Android TOTP apps and identified serious security vulnerabilities such as use of third party data, failure to meet cryptographic standards, and weak password recovery mechanisms like using SMS and email. According to a user survey of 330 individuals, it was found that most users were not aware of the risks even during cloud backups, lacked informed consent in cloud backups and a very large proportion of them did not even have an alternating mode of recovery. The results highlight a severe vulnerability in today TOTP practice and make it paramount to introduce transparent and user-controllable approaches to backup and recovery options to prevent account lockouts.

In order to overcome the identification of the shortcoming of JWT that does not take into account user behavior history, Ahmet Bucko , Kamer Vishi [7] proposes enhancement of traditional JWT authentication by incorporation of user behavior metrics to develop dynamic trust score. The system weighs conditions that include regularities of attempts to enter passwords, correspondence of IP addresses, and user agent type into an accumulative trust rating. Based on the C#, .NET framework, and PostgreSQL, this solution is highly effective in enabling reliable decisions on authentication

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

in the web applications since they offer a risk-based authentication validation. The paper shows enhanced security performance with the admission of some drawbacks such as intricacy in the calibration of scores as well as presumable privacy concern.

The study of Udban Dalimunthe, Emansa Hasri Putra [8] weight on the usage of JSON Web Token (JWT) as a secure authentication mechanism that will occur on various platforms without duplicating information systems. JWTs are designed to be secure and interoperable, use HMAC-SHA512 as the content integrity algorithm to sign the payload and have been implemented as cookies by browsers. The study shows the effective collaboration of JWT into various systems, displaying the comparisons of performance among HMAC-SHA256 and HMAC-SHA512. It has been observed that HMAC-SHA256 is a bit faster in serial tests whereas HMAC-SHA512 is faster in parallel tasks. Both algorithms are appropriate and depend on the execution environment and the network circumstances, but JWT + HMAC is very efficient, and light weighted approach to the secure distributed authentication.

Gayatri Bhamburkar [9], Yash Balkhande proposal of a three-tiered security architecture that is expected to provide better security to information and user authentication within a digital system. Some of the technologies that the model incorporates are JSON Web Tokens (JWT) to provide secure authentication and authorization, CryptoJS to encrypt, decrypt and hash sensitive data and NodeMailer to send one-time passwords (OTP). The initial level centers around conventional username / password authentication, creating an initial level of safety. The second-level dictates the consideration of Google CAPTCHA to rule out the possibility of automated attack and ensure that real individuals are talking to themselves. The final step is that of dynamic verification whereby an OTP is sent to the registered mobile number or email of the user. Before data is stored it is encrypted with the use of CryptoJS and thus adds greater degree of data confidentiality. This tiered system sets up a significantly increased level of security that encompasses multiple vectors of the threats in other words as well as secure yet convenient access to the systems and services.

Adei Arias, Cristobal Arellano [11] Although it has led to the disruption of industrial operations, on the down side of industrial internet of Things (IIoT), it has arrived with one of its core challenges; security vulnerability. These inherently IT-based, traditional SIEM products may not provide the capabilities necessary to address the peculiar challenges associated with IIoT, including volumes of data and demands of near-real-time response to threats. In order to take into consideration these shortcomings, the idea of incorporating Digital Twins (DT) virtual representation of physical assets into the SIEM is suggested. This integration will automate incident response in Operational Technology (OT) systems to be more effective in real-time threat detection, response effectiveness, and post incident process management. An account of a prototype implementation written out demonstrates the feasibility and efficacy of this sort of approach, giving evidence of the way in which it could be applied to holding the industry, and rendering the operations impervious to the new condition and dimension of threats.

In their article Malvin1, Cutifa Safitri [14] researchers talked of the problem of JWT (JSON Web Token) exposure, a scenario that occurs when the tokens used are exposed to the response header of web browsers allowing them to be stolen by lesser entities. It could lead to identity theft and the unauthorized access to APIs due to such leakage. To prevent this risk, this paper proposes a new method of enhancing the JWT security by segmenting the token and then encrypting both parts individually with RSA256 and finally rejoining separately encrypted tokens. This modified and coded token structure is difficult to determine and use by the attackers. The hijacked token is sent back into the response header and it remains functional as long as it becomes secure. The approach is proved to reinforce the web application protection significantly because now the tokens are not as accessible and are more difficult to misuse to optimize the security of user data

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

III. METHODOLOGY

FLOW DIAGRAM:

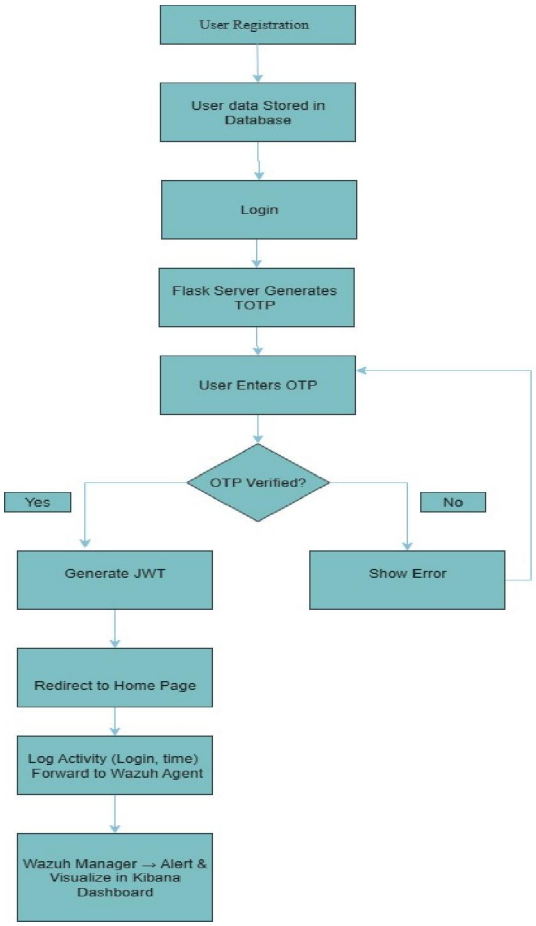

Fig 1. Flowchart of the system

This research adopts a layered and modular approach to design and implement a secure Multifactor Authentication (MFA) system using Flask, Firebase, and Wazuh. The primary objective is to enhance login security by combining email/password authentication with a time-based OTP The given research project considers a multi-layer and modular way to develop and run a secure Multifactor Authentication (MFA) system using Flask, Firebase, and Wazuh. The main target is to increase the security of the log in process using a mixture of email/ password authentication and a time based one time password system, along with implementing real time security monitoring and notification by Wazuh. The Flask backend hosts the code to handle user registration, user logging-in, the role-based access control (Admin, User, Guest), OTP generation using PyOTP and JWT-based session handling. Firestore and firebase authentication are utilised to have user data and the verification of the user identity securely. The users are also securely alerted about OTPs via OAuth2 on Gmail and there is no hardcoded credentials to use. Once OTP confirmation is done, a JWT is generated so as to give the users access to secured resources ensuring security. All authentication flows are fully tested, including error conditions and attack conditions are validated to be correct, efficient, and secure from attack vectors such as brute force or replay attacks.

Wazuh as a SIEM will be expected to provide higher-level threat, and system-monitoring capabilities to the Flask server. Wazuh agents monitor corruptions of files, logs of authentication, config files, and system-level events. Alerts are generated in real-time as suspicious activity (i.e., multiple failed sign on or unexpected file changes) is detected. The following alerts are shown and analyzed in the Wazuh dashboard with Kibana. Such integration provides more than

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, August 2025
Impact Factor: 7.67

visibility on authentication anomalies and user behaviors; it also helps with audit compliance and proactive security response to enhanced threats. As such the system provides high-fidelity multifactor authentication coupled with broader automated monitoring as required in a modern secure application.

IV. RESULTS AND DISCUSSIONS

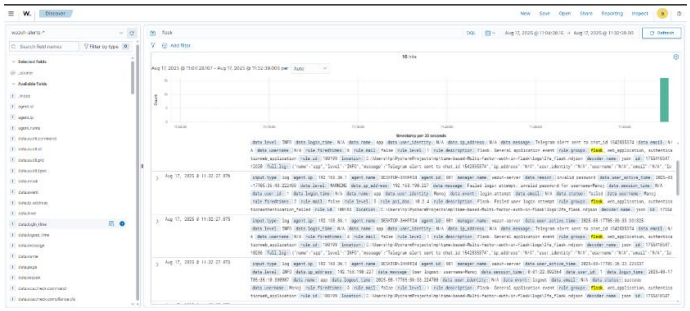

Fig 2 : Wazuh alerts Summary of MFA application

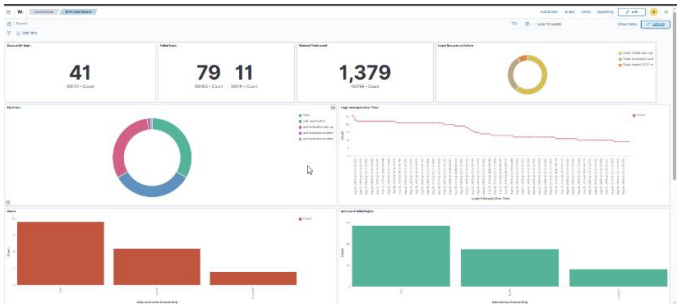

Fig 3: Real time logs shown in Wazuh Dashboard

The solution produced to allow Multifactor Authentication (MFA) was implemented with the aim of improving the level of security through a combination of password-based, along with time-based one-time passwords (TOTP): the latter were provided by Gmail via OAuth2, and Firebase maintained user information and their roles. It was confirmed that the registration, log-in and OTP verification take place normally with the unauthorised user being locked out successfully. The use of JWT sessions enabled secure navigation through them, and the OTPs worked with an expiry time to be able to dismiss the risk of replay attacks. This was indicated by the performance that there was minimal latency in the generational and validation of OTPs and that means that the program would require less interference with security. Wazuh integration made it possible to monitor anomalies in real-time and alert on repeated unsuccessful logins and brute-force attacks as well as unauthorized file updates, among others, and tabulate them in dashboards in Kibana. These results show that the specified MFA framework, with the addition of Wazuh analytics solution, can be practical and scalable enough to offer the necessary protection against the mainstream malicious threats and the security visibility continuity ensuring protection, thereby, being an adequate solution to utilize in the enterprise-level environments, as well as in compliance-oriented settings.

V. CONCLUSION

The given Multifactor Authentication (MFA) solution, which is vested into and integrated with Firebase, JWT, and Gmail-driven OTP validations supply a highly secure and easy-to-use protection solution against unauthorized access. With traditional password verification, and the incorporation of dynamic one-time passwords, the attack-surface of the system is greatly minimized with regards to credential thefts, and replay attacks. To further complement the solution, the Wazuh analytics are deployed so that real-time monitoring, abnormal behavior, and automatic notifications may be introduced, maintaining an overview of security events at all times. The experimental results proved that OTP delivery was reliable and that verification was accurate, and presented the malicious logins with minimum performance

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, August 2025 Impact Factor: 7.67

overhead. In a nutshell, this study confirms the efficacy of MFA with SIEM-driven analytics in providing authentication security, and it is therefore an acceptable strategy where authentication security is important in enterprise and cloud-based applications whose security needs to be upgraded in terms of user trust and data integrity.

REFERENCES

[1] Rakesh Bhavsar ,Vishvjit Thakar "Design and Implementation of an Open-SourceSecurity Operations Center for Effective Cyber ThreatDetection and Response" Research Square , https://doi.org/10.21203/rs.3.rs-5795888/v1, 2025
[2] Rafid S. Abdulaziz 1 "Resolve Problems Facing Application Programming Interfaces (APIS) In The Wazuh (SIEM) Solution" Anbar Journal of Modern Sciences, Vol. 1, No. 1, Feb. 2025.
[3] Dario Šuškalo, Zlatan Morić, Jasmin Redžepagić & Damir Regvart Comparative Analysis Of Ibm Qradar And Wazuh For Security Information And Event Management"doi:10.2507/34th.daaam.proceedings At International Symposium On Intelligent Manufacturing And Automation
[4] Diogo Donadoni Santos, Eva Rodriguez Luna "Cybersecurity Incident Response in eHealth" A Master's Thesis , Universitat Politècnica de Catalunya Barcelona, May 2023
[5] Honey Paptan , Deepanshu Garg ,Harsh Kumar ,Komal Mehta "Multi Factor Authentication System" , International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST), Volume 10, ISSUE 7 – July 2024
[6] Conor Gilsenan "Exploring the Security and Privacy Impacts of Using 2FA Apps" Technical report, University of California, Berkeley available on http://www2.eecs.berkeley.edu/Pubs/TechRpts/2025/EECS-2025-49.html, May 13, 2025
[7] Ahmet Bucko , Kamer Vishi , Bujar Krasniqi , and Blerim Rexha "Enhancing JWT Authentication and Authorization in Web Applications Based on User Behavior History", Computers 2023, 12, 78. https://doi.org/10.3390/computers12040078
[8] Syabdan Dalimunthe, Emansa Hasri Putra, Muhammad Arif Fadhly Ridha "Restful Api Security Using Json Web Token (Jwt) With Hmac-Sha512 Algorithm In Session Management", IT Journal Research and Development (ITJRD) Vol.8, No.1, August 2023
[9] Yash Balkhande, Gayatri Bhamburkar, Shreyash Waghmare, Vedant Nehare, Vijay Gadicha "Implementation of comprehensive information security model by using JWT & CryptoJS" DOI: https://doi.org/10.21203/rs.3.rs-3976233/v1 Feb 29,2024
[10] Mr. James Sani "Improved Log Monitoring UsingHost-based Intrusion Detection System", Advanced International Journal of Multidisciplinary Research, Volume 1, Issue 1, July – August 2023
[11] Adei Arias , Cristobal Arellano , Aitor Urbieta , Urko Zurutuza, "Leveraging Digital Twins and SIEM Integration for Incident Response in OT Environments" Journal of Neurointensive Care (JNIC) 2024, ISBN:978-84-09-62140-8
[12] Muhammad Syahreen1, Noor Hafizah2, Nurazean Maarop3, Mayasarah Maslinan4 "A Systematic Review on Multi-Factor Authentication Framework" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 15, No. 5, 2024
[13] Michaela Bergman "Login hardening with Multi-factor Authentication" MASTER´S THESIS, Department of Electrical and Information Technology Lund University , June 23, 2021
[14] Malvin1, Cutifa Safitri " JSON Web Token Leakage Avoidance using Token Split and Concatenate in RSA256" Indonesian Journal of Computing, Engineering, and Design (IJOCED), 2023, 5 (1); doi.org/10.35608/ijoced.v5i1.325
[15] Emerson Ribeiro de Mello1*, Michelle SilvaWangham2, Samuel Bristot Loli1, Carlos Eduardo da Silva3, Gabriela Cavalcanti da Silva4, "Multi-factor authentication for shibboleth identity providers, de Mello et al. Journal of Internet Services and Applications , 2020
[16] Wazuh, "Installing the Wazuh centralcomponents",Wazuh.https://documentation.wazuh.com/current/installation-guide/index.html. (accessed June 25, 2025).
[17]Wazuh,"AgentWazuh."https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html#wazuh-agent (accessed June 23, 2025).