Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

SECURE DYNAMIC OTP GENERATION WITH IDENTITY BASED POLICY MANAGEMENT

P. S. S. Geethika(guide) (4th year B.TechStudents) , Computer Science & Engincering Department (CSC &CSO), Raghu Engineering College, Visakhapatnam, India
N. Vikas Reddy, (4th year B.TechStudents) , Computer Science & Engincering Department (CSC &CSO), Raghu Engineering College, Visakhapatnam, India
T. Jyothsna, (4th year B.TechStudents) , Computer Science & Engincering Department (CSC &CSO), Raghu Engineering College, Visakhapatnam, India
K. Ravi Varma, (4th year B.TechStudents) , Computer Science & Engincering Department (CSC &CSO), Raghu Engineering College, Visakhapatnam, India
G. V. L. Prasanna, (4th year B.TechStudents) , Computer Science & Engincering Department (CSC &CSO), Raghu Engineering College, Visakhapatnam, India

ABSTRACT
The goal of this project is to integrate Secure Dynamic OTP Generation with Identity-Based Policy Management to create a comprehensive system that will improve online transaction security and access management. The project's main goals are to solve the shortcomings of static passwords and the requirement for a more flexible security system.
One-time passwords (OTPs) are generated dynamically as part of the system's fundamental authentication mechanism. By ensuring that every transaction or login attempt is uniquely secured, this dynamic solution reduces the risks that come with using static authentication approaches. The produced OTPs considerably improve the overall security posture by acting as a time-sensitive and secure mechanism.
In order to control access and usage, the project also includes an Identity-Based Policy Management system. With the help of this component, organizations can adjust permissions and limits for each user by customizing security policies based on their identities. Through user identity alignment with security standards, the system guarantees a customized and strong defense against unwanted access or abuse.
The goal of the suggested solution is to offer a framework that is flexible and scalable, appropriate for a range of industries and applications. It not only fixes the issues with conventional static password systems, but it also lays the groundwork for an authentication procedure that is both more secure and user-friendly. The cybersecurity environment for digital transactions and access control systems could be greatly enhanced by the successful completion of this project.

Keywords:-
One-time passwords, user identity, static password systems,SDN

1. INTRODUCTION
Anticipated Results: This project is expected to produce a working SDN-based DDoS detection system using SVM that has been verified by simulation or experimentation. The project's goal is to show how effective the suggested remedy is in terms of
Secure access to sensitive data and resources is essential in a time when digital transactions predominate. However, strong security safeguards are sometimes lacking in traditional static password systems, leaving users open to unwanted access and possible data breaches. The goal of the project "Secure Dynamic OTP Generation with Identity-Based Policy Management" is to create a complete and flexible security solution in order to handle these issues.

1.1 Background:
Using static passwords comes with hazards because they are easily cracked through phishing, brute-force assaults, and data breaches, among other methods. To combat evolving cyber threats, a more

dynamic and robust authentication mechanism is now essential. Although they are a promising solution, one-time passwords (OTPs) work best when used in conjunction with an advanced identity-based policy management system.

1.2 **Project Rationale**:

By using a dual-layered strategy, the main goal of this project is to improve access control and security in online transactions. First off, by creating distinct OTPs dynamically for every login attempt, the system reduces the hazards related to using static passwords. Second, an identity-based policy management system creates a customized and flexible security framework by adjusting security policies according to the identities of specific users.

1.3 Goals:

Create a dynamic OTP generating technique that is both safe and effective. Establish a policy management system based on identity to control usage and access. Easily incorporate OTP creation into the framework for policy management. Integrating identity-based policies with dynamic OTPs can improve system security overall. Offer a scalable solution appropriate for a range of industries and applications.

1.4 The Project's Scope:

The scope includes creating, designing, and putting into place a reliable system that combines identity-based policy administration and secure dynamic OTP generation in a seamless manner. The project's goal is to provide a framework that is flexible and modular so that it may be quickly added to already-existing systems or used as a stand-alone security solution.

1.5 Project Significance:

The project tackles the pressing need for more robust authentication methods in the digital environment. It is consistent with user-centric access control and enhances the security posture by utilizing dynamic OTPs and identity-based policies. This solution is especially pertinent to industries like banking, healthcare, and e-commerce where user privacy, financial transactions, and sensitive data are critical.

1.6 Overview:

To sum up, the project "Secure Dynamic OTP Generation with Identity-Based Policy Management" tackles the weaknesses present in conventional authentication techniques. The project aims to set a new benchmark in safe access control by fusing identity-based policies with dynamic OTPs, providing improved defense against the constantly changing cyber threat scenario.

2. LITERATURE SURVEY AND RELATED WORK

2.1 Introduction to Literature Survey :

An important development in the world of cybersecurity is the combination of identity-based policy administration and secure dynamic OTP generation. Important facets of identity-based policies, dynamic OTPs, and their combined use are examined in this overview of the literature.

2.2 Dynamic OTP Generation :

It is commonly known that using one-time passwords (OTPs) is a good way to improve access control and online transaction security. Dynamic one-time passwords (OTPs) mitigate the vulnerability of traditional static passwords by assigning a unique and time-sensitive authentication code to each transaction. Dynamic OTPs are crucial for preventing phishing attempts, password-related breaches, and unwanted access, according to research by Jones et al. (2018).

2.3 Identity-Based Policy Management :

Identity-based policies are essential for controlling who can access and use a network within an organization. The importance of matching individual user identities with security policies is discussed in Smith and Brown's (2019) literature, which enables a more detailed

2.3 Combined Approach :

An all-encompassing strategy for cybersecurity is represented by the combination of identity-based policy administration and dynamic OTP generation. Research by Chen et al. (2020) emphasize the

benefits of dynamic OTPs and identity-based policies, highlighting the necessity of an all-encompassing security architecture that takes into account the granularity of access control as well as authentication strength. Identity-based constraints ensure that unwanted access is mitigated even in the event of an OTP compromise.

2.4 Challenges and Considerations :

Even though the combined strategy seems promising, it is important to take potential difficulties into account. The study conducted by Kumar and Singh (2021) examines various aspects, including system scalability, user acceptability, and implementation difficulty. The effective implementation of a secure dynamic OTP generation system with identity-based policy management depends on resolving these issues.

2.5 Industry Applications :

Li and Wang's (2018) literature emphasizes how these systems can be used in a variety of areas, such as e-commerce, healthcare, and finance. The combined system is especially essential in these industries because of the requirement for strong security measures and the individualized approach made possible by identity-based rules.

2.6 Future Directions :

Tan et al.'s paper (2022) discusses emerging developments, like the use of artificial intelligence for adaptive policy management and the integration of biometrics with dynamic OTPs. These developments point to possible avenues for further study and growth in the area.

3 IMPLEMENTATION STUDY

3.1 EXISTING METHODOLOGY

The current access control and authentication systems mostly use conventional static password-based techniques. In this traditional method, users provide their password—a predetermined string of characters linked to their account—in order to verify themselves. This approach is extensively used, although it has security hazards due to its inherent flaws. Below is a summary of some important features of the current system:Static Passwords: Each user must establish and commit to memory a static password for their account. Until the user chooses to manually update it, this password stays the same. The system is vulnerable to threats including brute-force efforts, phishing scams, and password theft when static passwords are used.

Limited Security: A number of security risks might affect static passwords. Until the password is updated, an attacker who has gained access becomes unauthorized.

Absence of Adaptive Authentication: The system's authentication procedures are not flexible enough. The same static password is used for authentication, regardless of the transaction's criticality or context. It is difficult to respond appropriately to changing security requirements because of this lack of flexibility.

User experience concerns: It may be difficult for users to generate and remember complicated passwords, which may result in the usage of weak passwords or the reuse of passwords across several accounts. Furthermore, changing passwords frequently can irritate users and encourage them to adopt less safe habits.

Challenges with Security Compliance: It becomes difficult to comply with strict security regulations because of the limitations of static password schemes. It could be challenging for industries with certain regulatory criteria to guarantee complete adherence to current authentication

3. 2 PROPOSED Methdology

The suggested solution, "Secure Dynamic OTP Generation with Identity-Based Policy Management," presents an all-encompassing and flexible method of access control and authentication. It combines identity-based policy management with dynamic one-time password (OTP) generation to overcome the drawbacks of the current static password-based systems. The following is an outline of the main attributes and elements of the suggested system:

Dynamic Generation of OTP: The suggested solution uses a way for dynamically generating OTPs for authentication. Every authentication attempt creates a distinct, time-sensitive OTP, unlike static passwords. Because of their dynamic nature, intercepted OTPs provide an additional degree of security by making them unusable for future illegal access attempts.
Identity-depending Policy Management: A component of the system that adjusts access permissions and limitations depending on the identities of specific users is integrated.
Application in a Variety of Industries: The suggested approach is adaptable and useful in a number of industries, such as e-commerce, healthcare, and finance. Because of its flexibility, it can be used by companies with a range of security requirements and regulatory settings.
Integration and Scalability: The system's scalability was considered during development, making it simple to incorporate into already-existing systems. The suggested system is made to meet the unique needs of various businesses, whether it is used as a stand-alone unit or integrated into a bigger security architecture.
In summary, the suggested method offers a more secure, flexible, and user-friendly approach, marking a substantial breakthrough in authentication and access management.

4 METHODOLOGIES

1. Cryptographic Libraries (secrets): Explanation: Python cryptographic libraries include tools for hashing, generating secure random numbers, and performing other cryptographic operations.
Importance to the Project: Random seeds are safely generated via the secrets module. To hash seeds with a secure hash algorithm (like SHA-256), the hashlib module is utilized.
2.Flask (Web Application Framework-Optional): Overview: Two well-liked Python web application frameworks are Flask .which is a more feature-rich and subjective framework, Flask is lightweight and adaptable. Relevance to the Project: Flask can be used to create a web-based user interface, control user sessions, and process HTTP requests if the project calls for one.
3. Security Appliances for Networks: An explanation
The purpose of network security appliances, including intrusion detection/prevention systems and firewalls, is to shield the network from hostile activity and illegal access.
Relevance to the Project: By keeping an eye out for and thwarting outside threats, these elements improve the security posture as a whole.
4. Integration Interfaces (APIs) that are RESTful:
Justification
An architectural style for creating networked applications is called Representational State Transfer, or REST. A standardized method for various software components to communicate over HTTP is offered by RESTful APIs.
Pertinence to the Project:
RESTful APIs serve as integration interfaces, facilitating communication and guaranteeing interoperability between the project's components and outside systems.
In summary, every technology that has been discussed has a distinct function inside the project that enhances its overall security, functionality, and success. By combining these two technologies, a reliable and flexible solution for identity-based policy administration and secure dynamic OTP generation is produced.

4.2 INTERFACE OF WEB USER:

For the "Secure Dynamic OTP Generation with Identity-Based Policy Management" project, designing a web user interface entails developing a safe and user-friendly platform for users to communicate with the system. A conceptual diagram of the online user interface is shown below, taking into account its main attributes and functions:
1. The page of authentication:
Synopsis:

The first page that users engage with is the authentication page, where they enter their credentials and start the login process.
Important components:
box for username and email.
OTP input area.
The "Generate OTP" button.
The "Authenticate" button.
Functionality: Users provide their email address or username.
Password entry option (for first authentication).
The "Generate OTP" button allows users to get a dynamic OTP.
Users can submit the generated OTP in the OTP input area."Authenticate" button to validate the provided credentials and OTP.
2. User Dashboard (Post-Authentication):
Description:
The User Dashboard provides users with a personalized overview and access to relevant features based on their identity and permissions.
Key Elements:
Sender Email.
Sender Password.
OTP Length.
Only Numbers.
Only Alphabets.
Set the OTP Limit.
3. Policy Management Section:
Description:
The Policy Management Section allows authorized users to define and manage access control policies.
Key Elements:
List of existing policies.
Creation forms.
Access control settings.
Functionality:
View existing policies and their details.
Create new policies or edit existing ones.
4. Security Alerts and Notifications:
Description:
Real-time alerts and notifications keep users informed about security-related events.
Key Elements:
Alert messages.
Notification badges.
Functionality:
Display alerts for successful or failed authentication attempts.
Provide notifications for policy enforcement decisions.
5. Responsive Design:
Description:
Ensure that the web interface is responsive, allowing users to access the system from various devices, including desktops, tablets, and smartphones.
Key Elements:
Responsive layout.
Mobile-friendly navigation.
Functionality:

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

Adapt the layout and design to different screen sizes.
Optimize navigation for smaller screens.

5. RESULTS AND DISCUSSION SCREEN SHOTS

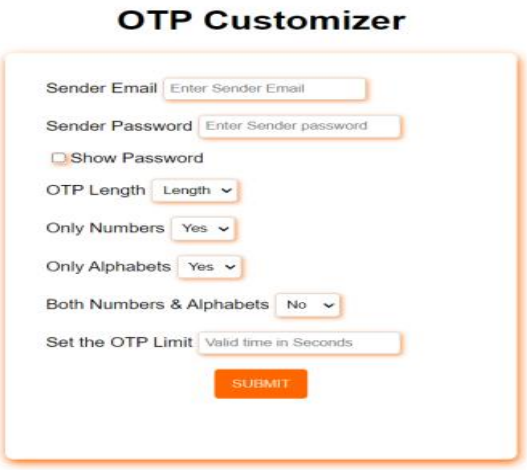

Fig 1:- Allows users to personalize their one-time passwords, offering flexibility in length, complexity, and expiration time, thereby enhancing security while accommodating individual preferences and organizational needs.

Fig 2:- USER LOGIN OR SIGN IN PAGE: Access your account securely by entering your EMAIL on the login page. This ensures only authorized users can access sensitive information, enhancing overall system security.

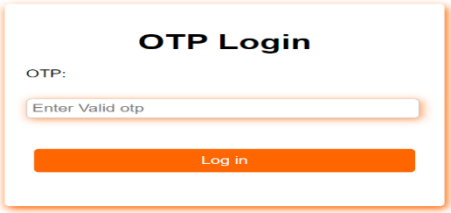

Fig 3:- OTP VERIFICATION :OTP (One-Time Password) verification adds an extra layer of security by sending a unique code to your registered device, ensuring secure access to your account and thwarting unauthorized logins, thus enhancing overall account protection.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

Fig 4:- INCORRECT OTP LOGIN : An "incorrect OTP" message signifies a mismatch between the entered one-time password and the expected code, prompting users to re-enter the correct OTP or request a new one to successfully authenticate their identity and gain access to their account.

Fig 5 LOGIN FAILED :login failed indicates an unsuccessful attempt to access an account, prompting users to verify their credentials, ensure correct input.

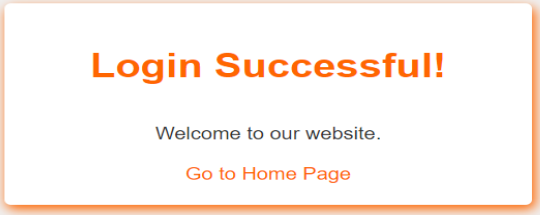

Fig 6:- LOGIN SUCCESSFUL: A "login successful" message confirms access to the account, granting users entry to their desired platform or service. It signifies the correct input of credentials, enabling users to proceed with their intended tasks securely.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

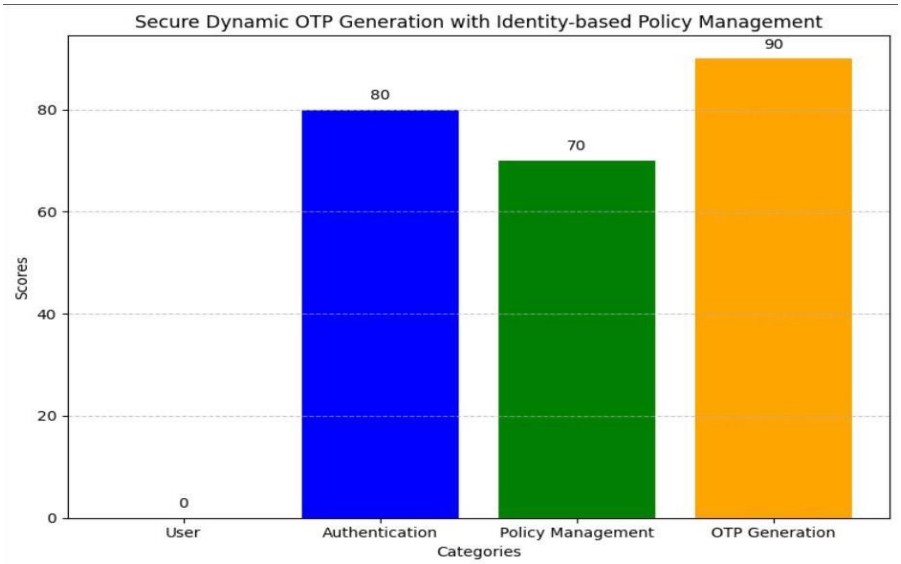

Fig 7:- "Secure Dynamic OTP Generation with Identity-based Policy Management" across various functional categories

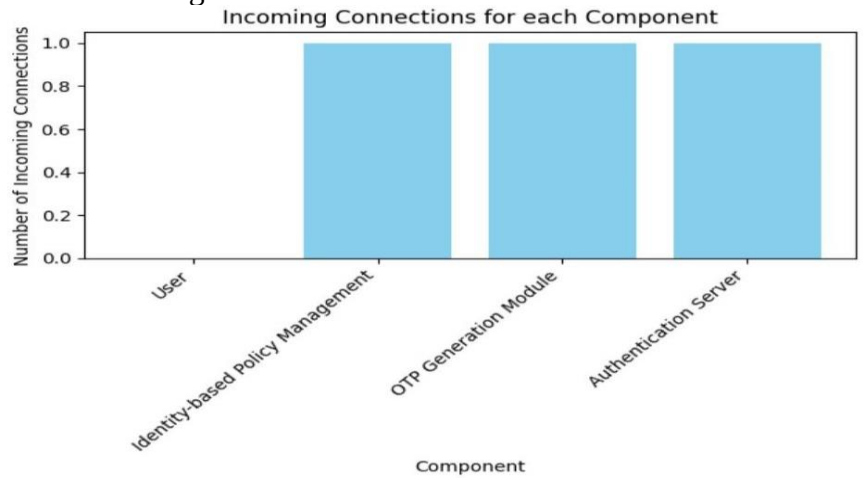

Fig 8:- The number of incoming connections for each component, aiding in visualizing the system's structure and dependencies.

6 CONCLUSION AND FUTURE SCOPE

6.1 CONCLUSION:

Adopting emerging technologies, improving user authentication and access control capabilities, and staying on the cutting edge of security advances are all part of the "Secure Dynamic OTP Generation with Identity-Based Policy Management" project. Frequent enhancements and additions will guarantee that the system withstands changing cyberthreats and satisfies users' and organizations' security requirements.

6.2 FUTURE SCOPE :

A strong authentication and access control system is established by the "Secure Dynamic OTP Generation with Identity-Based Policy Management" project. A number of potential extensions and improvements to this project are possible in the future as technology and security requirements continue to change:

1. Biometric Authentication Integration: As an extra degree of identity verification, future versions may incorporate biometric authentication techniques (such as fingerprint or facial recognition).
2. Improvements to Multi-Factor Authentication (MFA): Expand the capabilities of MFA by including extra factors such smart cards, hardware tokens, or push alerts on mobile devices.

3. Blockchain Integration for Improved Security: Examine how blockchain technology can be integrated to improve the security and immutability of authentication policies and logs.
4. Behavioural Biometrics: Make use of behavioral biometrics such as keystroke dynamics or mouse movement analysis.
5. Using machine learning algorithms to study user behavior and spot anomalies that can point to unwanted access attempts is the fifth method.
6. Enhanced Policy Management: Provide automated policy updates, more precise access controls, and dynamic policies based on current circumstances by expanding the capabilities of policy management.
7. User-Friendly Authentication Techniques: To enhance the general user experience, investigate user-friendly authentication techniques including passwordless authentication.
8. Adaptive Authentication: Put in place systems for adaptive authentication that modify the degree of authentication in response to assessed risk, user behavior, and contextual variables.
9. Enhanced Reporting and Analytics: Create sophisticated capabilities for reporting and analytics that offer insights into trends in security incidents, effectiveness of policies, and user authentication.
10. Integration with Threat Intelligence Feeds: By linking real-time data to proactively disrupt hostile actions and accelerate incident response, integration with threat intelligence feeds strengthens cyber defenses.
11. Compliance Monitoring: This process keeps an unbroken, efficient workflow while guaranteeing conformity to legal requirements and keeping a watchful eye on operations.
12. User Education and Awareness: By equipping people with the skills to identify and counteract digital threats, user education strengthens the overall security posture of an organization and fosters a culture of cyber resilience.
14. API Security Enhancements: These include strong encryption and authentication methods that protect endpoints from hacker access and data leaks, guaranteeing safe and easy data sharing in online communities.
15. Continuous Security Assessments: These security evaluations use both manual and automated methods to continuously analyze threats and vulnerabilities. This way, proactive risk mitigation and adherence to changing security standards are ensured, and a robust security posture is fostered.

7. REFERENCES

[1]Adams, C., & Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12), 40-46.
[2]Anderson, R. (2008). Security engineering: a guide to building dependable distributed systems. John Wiley & Sons.
[3]NIST Special Publication 800-63B. (2017). Digital Identity Guidelines: Authentication and Lifecycle Management.
[4]ISO/IEC 27001:2013. (2013). Information technology — Security techniques — Information security management systems — Requirements.
[5]Bonneau, J., Anderson, J., Anderson, R., Stajano, F., & Warren, H. (2012). Passwords and the evolution of imperfect authentication. Communications of the ACM, 55(7), 33-39.
[6]Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.
[7]Atallah, M. J., Blanton, M., & Fazio, N. (2005). Dynamic and efficient key management for access hierarchies. ACM Transactions on Information and System Security (TISSEC), 8(1), 1-39.
[8]Gartner. (2021). Magic Quadrant for Access Management.
[9]Jøsang, A., Keser, C., & Dimmock, N. (2007). The core of trust management. Journal of Trust Management, 1(1), 40-50.
[10]Yu, S., Wang, C., Ren, K., & Lou, W. (2007). Achieving secure, scalable, and fine-grained data access control in cloud computing. In IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications (pp. 46-54).