RESEARCH ARTICLE OPEN ACCESS

Cloud Based OTP Brute Force Blocker

Yamuna Rupini J,Andal S

Computer Science, Francis Xavier Engineering College, Tirunelveli – TamilNadu-India
yamunarupinij.ug22.cs@francisxavier.ac.in

Computer Science, Francis Xavier Engineering College, Tirunelveli – TamilNadu-India
andal@francisxavier.ac.in

Abstract:

The cloud-based reliable authentication platform with innovation in security analytics offers various defensive features like user behavior based OTP verification, intelligent bot detection and behavior based adaptive counter measures against advanced cyber-attacks in a convenient web authentication environment. To achieve this, we leverage next-generation behavioral analysis techniques to accurately track user interactions, capturing metrics such as typing speed, response time delays, frequency of corrections, and input characteristics during the OTP validation procedure. The intelligent authentication system doesn't just check for code accuracy at its core like standard authentication solutions but it adds an additional layer of human-centric cognition by presenting seemingly complex OTP challenges coupled with real-time instructions for entering characters (such as entering only digits, selecting elements based on position in a string, etc.) requiring critical interpretation before submission. The byproduct of this method is a supremely secure alphanumeric token transformed into visual instruction puzzles necessitating human logic to interpret (e.g., number extraction, position-based selection) thus significantly obstructing malicious automation tools or brute-force spam bots from breaching. Moreover, the platform implements a clandestine security feature utilizing web application stealth honeypot fields set in autogeneration mode within the login form. These invisible fields lure bots into common automation traps filling all fields so the platform can rapidly 'snitch out' attacker IP addresses and take proactive steps to blocking them motion etching their identity solely using field extension detection. Additionally, the server actively monitors user interaction patterns and assigns confidence scales for human, attacker, and attacker automated classifications to authenticate multiple user verification attempts while preempting, deceiving, or falsifying automation. Authentic persistent users are granted several authentication recompilations with permissible time delay restrictions; in contrast, hostile behavior quickly emanates into immediate enemy status enrichment by instant moment effect deviation and session rejection. At every instant, all perils are indexed and summarized in a secure elastic cloud tracking environment giving admins what intelligence is needed to inherently stay ahead of evolving criminal tactical innovations.

Keywords —**Cloud-Based Authentication, Human-Aware OTP, Bot Detection, Behavioral Authentication, Cyber Attack Prevention, Honeypot Security, Intelligent OTP Verification, IP Blocking, Adaptive Security Systems, Secure Web Authentication.**

I. INTRODUCTION

In today's net-world, secure login/authorisation/authentication has become irrefutably essential as the number of web-based services boom across all possible domains including banking, cloud computing, e-commerce, digital identities etc. The rapid proliferation of net-based financial and personal transactions have inadvertently increased the number of security loopholes/attack vectors such as brute-force attacks, automated bots, theft of

credentials, loss of secret passwords, OTP based attacks etc., and made the traditional password based or weak authenticators an easy target to sophisticated attackers who unleash huge computing blasters and high speed scripts to exploit these weaker systems. These holes not only leave web users vulnerable to the malicious cybercriminal "inhibodent", but also de-authorise otherwise robust methods of conducting online transactions and activities. Existing OTP-authentication systems majorly concern on the validation of a passed user-OTP to the generated OTP, and do not dwell on how the attacker interacted with the system. In such systems, the attacker can keep reiterating various OTP combinations by using aggressive scripting in conjunction with high speed machines within the constraints of OTP validity, something which conventional security measures such as a fixed number of login attempts, resolving a CAPTCHA, or time-out lock-outs are not evidently sufficient to thwart. "Nothing in life is static" in the context of security, which limits the static security measures, making the system vulnerable against dynamic and distributed automated cyber-enemies. Static security counters, comparative to evolving attacker strategies, are impinged to find out suspicious trends in the hardware, network, web-application, and user-behavior at runtime. Moving a step ahead, intelligent authenticators should bag cloud computing, behavioral intelligence and adaptive security mechanisms to cast suspicions on the attacker behavior of usage.

II. ALGORITHMS

The core functionality of the proposed Cloud-Based Human-Aware OTP Attack Blocking System relies on intelligent algorithms. The intelligent algorithms play an important role to provide secure login/authentication, analyze user interactions intelligently, and implement Automated attack detection & real-time proactive attack detection to identify malicious login attempts. While the conventional OTP verification system verify only correctness of the input OTP, the proposed system use multi-layer of intelligence algorithms which analyze user behaviors, automatically identify attacks using bot and attacker detection algorithms. The algorithms keeps track of behavior parameters like, interaction time between user and OTP device, login time, attempts to enter OTP, OTP user have followed, Paranoia level, Honeypot interaction traces, to categorize attacker or legitimate user or bot attack using intelligent behavioral modeling, adaptive OTP challenge, risk based classification method. The proposed algorithms also allow response strategy implementation like cool-down period response, ip blocking, Honeypot decoy, etc.

A. Human Behaviour Analysis Algorithm

Based on the synthesized human behavioral patterns, The Human Behavior Analysis Algorithm aims to analyze the behavioral characteristics of users on the authentication UI, to verify if the user activity derives from a human user. During theOTP verification phase, the algorithm constantly analyzes the gesture signals, including you typing time gap, the number of back space correction, total typing delay time after instruction displayed and so on.

These behavioral symptoms give us some pointers regarding the steps followed by the human mind while reading the instructions and providing data manually. Real users tend to display natural natural thinking delay while reading the instruction OTP, make sporadic typing errors which get corrected and generally type at a moderate speed while providing the response.

Compared to this, responses from automated bots are usually instantaneous and occur without delay. When genuine failure responds, the responses are revealed to take less than a second for the whole value of the input, and correction behaviors are almost non-existent. Bots are unlikely to mimic this behavior, nor do they make use of natural pauses due to input being derived programmatically. Trapdoor based attacker works will seem to have rapid repeated inputs indicating there is scripting behavior.

From these interaction parameters, behavioral confidence scores are produced by the detection algorithm-an overall index of the probability that the requesting user is in fact human. The server uses these scores as the input to a classification engine to decide the message to present to the user.

B. Introduction Based OTP Validation Algorithm

This Instruction-Based OTP Validation

Algorithm takes OTP authentication a step further by turning it from a literal login process into an instruction based cognitive test. Rather than instruct the user to simply enter the entire OTP, this algorithm outputs a random alphanumeric string and current instruction.

For example, instructions to the user may be to just input the numbers in the OTP, retrieve characters at certain positions, or to enter say the even characters of the OTP. Here the user has to accept the challenge and figure out the answer based on the OTP.

After the user submits the answer, the algorithm internally computes the OTP output generated and applies the same instruction to see the expected output. The input submitted is then compared with the expected value to check if it is correct. If the response also matched the pattern, the check step is correct.

This makes the system much more secure because most automated scripts /bots send the whole OTP number itself. Since a bot cannot understand such instruction based interactions and pass through reasoning, this OTP instruction based authentication mechanism would stop all such bypass attempts.

C. HoneyPot Bot Detection Algorithm

Honeypot Bot Detection Algorithm The Honeypot Bot Detection Algorithm is a reputation system which detects automated bot activities by placing traps for bot detection in the system authentication page. It places some hidden form elements including hidden OTP text box and fake data entry areas which cannot be identified by the human users of the page, but can be identified by the webpage.

During form submission, the algorithm constantly watches these hidden fields. When bot interaction is detected in any of these honeypot fields, it instantly recognizes it as an automated bot. It then executes a series of counter measures including blocking the source IP, end the auth session, and log the bot activity in cloud security logs.

The detection system based on honeypot is one of the best, because this system is very quiet and no other action from the users is needed. This cannot be said of for example verification systems based on the use of captchas, requiring action from the genuine user, while honeypots just work in the background with bot behavior.

D. Attacker Pattern Detection Algorithm

This Attacker Pattern Detection Algorithm aims to find the attacker that is trying to get an unauthorized break-in through the brute-force or guess method (repeatedly). This algorithm will consider the time (in second) elapsed, no. Of failed OTP, no. Of auth requests, various indicators such as response time, no. Of instructions, no. Of instructions based OTPs, etc.

When a user makes numerous wrong guesses or has given the wrong information multiple times on guessing the combination (manual brute-force), it is detected by the system. Instead of blocking the user right away, it can activate a deception based defense. It generates an authentication success response in the front that seems the user is now authenticated but not granted access to the system actually and the user is logged and traced secretly.

E. Risk Scoring and User Classification Algorithm

The Risk Scoring and User Classification Algorithm-This component is the core decision engine of the authentication system. It takes input from the behavioural analysis, OTP verification, honeypot identification and attacker behavior pattern analysis modules and provides a final classification for user interaction. The algorithm combines all the values that would act as security inputs (behavior confidence score, number of failed attempts, honeypot presence status, response rate, whether OTP is followed or not etc) for a user login and assigns a dynamic risk score. This score represents how probable it is for the user interaction to be an attack. The system then classifies the user in to three types based on this risk score: Human, Attacker, or Bot. For human interactions, the system still imposes limitations on further tries via a temporary cooldown phase before allowing them to try authentication again, if the number of attempts exceed the threshold. For attacker pattern inputs, the deceptive honeypot strategy is initiated and for bot interactions, confirmed by either honeypot triggers or robotic interaction methods, the IP address of the source is immediately blacklisted

and session is terminated.

III. PROPOSED SYSTEM

The proposed Cloud-Based Human-Aware OTP Attack Blocking System is a smart authentication method to improve the comprehensive security of traditional OTP verify system by applying behavior analysis, adaptive dynamic authentication challenges and fully automated attack detection and classification mechanisms. Traditional OTP verify system only determines the accuracy of information input which exposes the system vulnerable to brute-force attack, attack by automatic system, repeated guessing and others. To overcome the above drawback, proposed human aware authentication system verifies the correctness of response with respect to generation of OTP as well as the behavior of human while verifying the OTP. The authentication system generates an even complex alphanumeric OTP and interact the user by instruction based challenges so that user needs to understand the instruction and supply the OTP part as the response rather than behavior human in a sense of partial input. Therefore, the user will undergo the cognition process before providing the response that makes feasible even for human to fool and impossible for automation tool to response in a short time. Over and above the simple OTP validation, the proposed system also provides expressive behavioral analysis by monitoring the time of response submission, number of incorrect guesses, deletion rate and delay time to check whether the person interacting with the system acts a human bot. The introduced association naming also make the system human aware that consists the honeypot attack by bot detection, attacker behavior detection and system administrator intelligent classification techniques. In the pattern analysis, a number of behind boxes called as targets are hidden inside the responded form of login to differentiate the attacking bot that interacts with every provided form field and bounces that releases large set of fake submitions into attacker environment. If the cobbled interactions on each behind hidden box, the identity of attacker defines as bot environment and the source host IP address is bumped within a fraction of second.

IV. WEB AND MOBILE PLATFORM BASED

The authentication system as mentioned above is a web based system with a cloud helper architecture which can been seamlessly integrated with new web systems, mobile services or digital services that require secure authentication of individual users. Interface mainly consists of a web based light weight and user friendly system where individual user submits his registered email or mobile number so that system can generate OTP and shows an instruction based challenge on the screens which guides the individual user to submit the section of password by following the instruction given.

I have ensured the frontend is as simple, user friendly and responsive as possible so that real users who get directed to it will be able to easily grasp what needs to be done. There are also hidden honeypot form fields in the form and background scripts that are monitoring user behaviors and detecting automated form submission to make sure the security measures do not adversely affect the user experience.

The backup is provided by cloud systems on the backend supporting the OTP generation, behavior analysis, user classification and security log. The cloud computing facilitates the hourly scalability of the system and the protection of authentication logs and attack records, as well as users' interfaces. A dashboard is available for the administrators showing the authentication trend, suspicious Login-ID pair, blocked IPs and security statistics.

V. AI-BASED HUMAN BEHAVIOR AND THREAT DETECTION

The proposed system uses artificial intelligence (AI) based behavioral analysis of human-computer interaction to determine whether the login is being initiated by a real human, attacker or a bot. In contrast to traditional OTP-based systems which simply verify the

accuracy of the code entered, proposed system analyzes behavioral cues and interaction patterns during the login process to authenticate the login attempt. The system analyzes various parameters such as keying speed, delay time, correction-counts, number of login attempts to determine whether interaction resembles human characteristic. A machine learning based pattern analysis mechanism would give a behavioral confidence level, which would aid in classifying whether the login attempt is made by a human, attacker or a bot. The system can learn user interaction patterns over time, and optimize detection mechanisms to reduce false positives and increase authentication security.

VI. INTEGRATED INTELLIGENT AUTHENTICATION RESPONSE

The system employs a hybrid response to various types of authentication behaviors. In the case of valid human users, the number of login attempts will be limited, and a post-I attempt delay will be issued to dissuade brute-force terrorists if the attempts are repeated beyond a threshold. In a situation where the attacker is making repeated invalid attempts, the response will be to identify the attacker behavior and to activate the honeypot deception response to disorient the attacker, while not enabling access; the response to automated bots is the detection of hidden honeypot fields and abnormal timing and actions, leading to an immediate banning of the IP address.

VII. SECURE CLOUD MANAGEMENT AND CLOUD LOGGING

Handling sensitive authentication data and login activity records Cloud based secure data management. The system archives all authentication data, behavior scores, user rating and security actions on the cloud. Our secure communication protocol with strong encryption scheme guarantee encryption of login data in transit and storage. The cloud infrastructure allows the system administrator to easily monitor the authentication activity, attack pattern, and to enhance the security policy over time.

VIII. INTELLIGENT USER CLASSIFICATION SYSTEM

The system is designed to intelligently classify an auth attempt into three categories: Human, Attacker and Bot. This classification is done by examination of various factors; on the basis of behavior (i.e. Correct instructions for OTP, response time and interaction with honeypots). Normal users usually act normally, with normal instructions of OTP and normal response time, while attacker guesses repeatedly and bot interacts by presence of Honeypots or RTC and instantly.

IX. USER SECURITY AWARENESS AND INTERACTION GUIDANCE

Guidance and Instructions, Feedback:The platform provides guidance and instructions for users throughout the login and OTP verification process about OTP challenges, authentication attempts, and security notifications. It educates users about secure login practices, potential indicators of malicious activity, and appropriate handling of the OTP credentials.

Through the use of the system login screen, users are made aware when an abnormal activity occurs while using authentication, offers instructions on how to attempt retry following a cooldown period, recognizes a trusted device and analyzes personal user activity to reduce accidental lockouts without compromising the security of protecting the system from unwanted intruders.

X. TECHNOLOGY

The designed authentication platform combines the latest Web 2.0 standards with intelligent security controls to implement a strong adaptive authenticator. During OTP verification, the system applies behavior analysis algorithms and rule-based classification to identify human, malicious and bot in the automated systems.

The cloud infrastructure is the storage of login logs, behavioral information, and security information, providing improved monitoring and analysis of data flow. The system uses the OTP generated based on dynamic pathway, together with instructions on cognitive question, thereby requiring realization from users.

By leveraging automated behavior detection, cloud and local services, and adaptive OTP validation, the authentication process is designed to provide a secure, scalable, and effective automated attack monitoring and response system. Whitelisting, account lockout policies, and spam protection all form part of the AuthN process. Other innovative use-cases include advanced honeypot detection, cool-down control policies and behavioral scoring services.

XI. EXPECTED BENEFITS

The proposed system strictly improves the security measures of one-time password (OTP) login system, human aware validation, behavior intelligence and automatic attack detection system help near to perfect. The three new systems reduce the chances of brute-force attack, blind access through automated programs and tedious confirmation process respectively. Combining the intelligent behavior recognition system with the adaptive security response system achieve strong security and user friendliness at the same time. The cloud computing infrastructure allows the system to be scalable, attach resistant and capable of real time attack detection and respond to attacks.

XII. RESULTS AND DISCUSSION

Based on the constructed system, we have witnessed proper operation of the Cloud-Based Human-Aware OTP Attack Blocking System with experimental tests. Although the system can be penetrated either by human attackers attempting repeated guesses or by intelligent bots, the detection and blocking of such attack behaviors can be revealed. In particular, the legitimate human users are confirmed and successfully authenticated by analyzing different behavioral patterns and OTP interaction logics, attack behavioral patterns from such reconnaissance attacks like repeated way back guessing attacks can be discovered and prevented by administering slow down timeouts or trap honeypots, while intelligent and password-reverse-knowledge mass attacks from computation bots can be instantly blocked by embedded honeypot triggers and abnormal interaction logs with high behaviors' generation speed. In conclusion, results from aforementioned exercises provide compelling evidence that intrinsic security combined with behavioral authentication can greatly strengthen current OTP-based authentication toward to human-aware authentication.

XIII. CONCLUSION

In conclusion, the proposed Cloud-Based Human-Aware OTP Attack Blocking System presents a promising authentication system that elevates OTP security with behavioral cues, an intelligent verification system and automated attack identification. This design incorporates intelligent algorithms, honeypot-guided bot detection mechanisms, and cloud-based monitoring components to efficiently identify human users versus bots on a network and any ABM attacks as they happen.

REFERENCES

[1] Y. Fujii, “Smartphone-Based Sensing Network for Emergency Detection: A Privacy-Preserving Framework for Trustworthy Digital Governance,” *Applied Sciences*, vol. 16, no. 2, Art. no. 1032, 2026.

[2] S. Dhivya, R. Ramnath, C. Redhanya, S. Sasi, and S. S. Priya, “Voice Recognition Powered Women’s Safety App,” *International Journal of Computer Science and Engineering*, vol. 10, no. 2, pp. 17–21, 2022.

[3] S. Shankar Pawar *et al.*, “RescueNow: Real-time SOS and Predictive Women’s Safety System,” *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, 2025.

[4] R. Priya, C. S., S. M., U. Parameshwaran, and T. S., “Safe Alert App,” *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, 2025.

[5] A. Jothi V. P., “AI-Powered Woman Safety Application with Real-Time Audio-Based Trigger and Emergency Alert System,” *International Journal for Multidisciplinary Research (IJFMR)*, 2025.

[6] K. S. and U. M., “AI-Based Personal Safety App with Adaptive Threat Detection,” *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, 2026.

[7] M. Ara and N. Rajeshwari, “AI-Based Women Safety and Alert System Integrating Multi-Channel Communication and Real-Time Location Tracking,” *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, 2026.

[8] P. Krishna Aghao *et al.*, “Suraksha Sathi: An Innovative SOS Application for Personal Safety Using Mobile Platforms and Location-Based Alerts,” *Recent Trends in Electronics and Communication Systems*, vol. 11, no. 03, pp. 27–40, 2024.

[9] T. S. and S. R., “Threat Eye – An Application of Safety Alert System for Real-Time Threat Detection Using Mobile Speech and NLP,” *International Journal of Scientific and Engineering Research (IJSER)*, vol. 13, no. 2, 2024.

[10] R. Pitchandi, “Smart Emergency Alert System Using Shake Detection and Location Tracking for Android Devices,” *Power System Technology Journal*, vol. 43, no. 3, pp. 2521–2530, 2019.