Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 45 No. 2
February 2024

Authentication Techniques in eProcurement System: A Review Paper

[1] Saru Chandrakar*, [2]Dr. Ani Thomas

[1]M.Tech. Student, Information Technology, BIT Durg

[2] Professor& HOD, Information Technology, BIT Durg

Abstract

E-government can give citizens superior and more helpful administration as restricted to conventional government administration. Utilizing an electronic approach in completing an acquirement handle opens up a part of issues with respect to security. The Straight forward nature of the method in hand is requiring a modern security framework. Unauthorized access gets to or distinctive interruptions sorts are showing an authentic danger. Threats include unauthorized access, data leakage, malicious codes, phishing, etc. An effective response to cyber attacks either natural or human-induced harms requires quick investigation of compromise and other information obtained both sometime recently and after the attack. Such data will empower crisis reaction administration in anticipating the attack quickly and rerouting activity proficiently. Moreover, recuperation endeavours depend on the procurement and investigation of opportunities knowing of the assault and sort of assault that might show the nearness of the back entryway, malevolent code, etc. Diverse confirmation strategies and caution frameworks in frameworks and databases containing base data that can be quickly upgraded will help of sparing misfortunes and lessening costs. This review paper in brief, presents the different authentication techniques in eProcurement system.

Keywords: Authentication, cyber criminals, cyber attacks, malicious codes.

1. Introduction

Authentication is the method of distinguishing users that helps in getting a framework, organization gadget. Get to control regularly decides client personality agreeing to qualifications like username and watchword. Other confirmation advances like biometrics and confirmation apps are moreover utilized to authenticate user identity.

User confirmation could be a strategy that keeps unauthorized clients from getting to delicate data. For illustration, Client A as it were has got access to important data and cannot see the critical data of Client B.

1.1 Different Authentication Techniques

1.1.1 Password-based authentication

Passwords are the foremost common strategies of authentication. Passwords can be within the shape of a string of letters, numbers, or special characters. To secure yourself you wish to make strong passwords that incorporate a combination of all conceivable choices.

Be that as it may, passwords are inclined to phishing assaults and awful cleanliness that debilitates viability. An normal individual has almost 25 distinctive online accounts, but as it were 54% of clients utilize diverse passwords over their accounts.

The truth is that there are part of passwords to remember. As a result, numerous individuals select comfort over security. Most individuals utilize straightforward passwords rather than making dependable passwords since they are less demanding to keep in mind.

The foot line is that passwords have a part of shortcomings and are not adequate in ensuring online data. Programmers can effectively figure client qualifications by running through all conceivable combinations until they discover a coordinate.

1.1.2 Multi-factor authentication

Multi-Factor Authentication (MFA) is a verification strategy that requires two or more free ways to recognize a client. Cases incorporate codes created from the user's smartphone, Captcha tests, fingerprints, voice biometrics or facial recognition.

MFA verification strategies and advance increment the certainty of clients by including different layers of security. MFA may be a great defense against most account hacks, but it has its pitfalls. Individuals may lose their phones or SIM cards and not be able to create a confirmation code.

1.1.3 Certificate-based authentication

Certificate-based verification innovation distinguishes clients, machines, or gadgets by utilizing advanced certificates. A computerized certificate is an electronic archive based on the thought of a driver's permit or an international id.

The certificate contains the computerized character of a client counting an open key, and the advanced signature of a certification specialist. Computerized certificates demonstrate the following:

a. Possession
b. Ownership
c. Proprietorship
d. Possession

of an open key and issued as it were by a certification specialist.

Clients give their advanced certificates when they sign in to a server. The server confirms the validity of the computerized signature and the certificate specialist. The server at that point employs cryptography to affirm that the client includes a adjust private key related with the certificate.

1.1.4 Biometric authentication

Biometrics verification may be a security advantage that depends on the special organic characteristics of an person. Here are key focal points of utilizing biometric confirmation innovations:

Natural characteristics can be effectively compared to authorized highlights spared in a database.

Biometric confirmation can control physical get to when introduced in entryways. You can include biometrics in your multi-factor confirmation process. Biometric verification innovations are utilized by customers, governments, and private organizations counting airplane terminals, military bases, and national borders. The innovation is progressively embraced due to the capacity to attain a high level of security without making ground for the client. Common biometric confirmation strategies incorporate:

Facial recognition—matches the distinctive confront characteristics of a person attempting to pick up get to an affirmed confront put away in a database. Confront acknowledgment can be conflicting when comparing faces at distinctive points or comparing individuals who see comparative, like near relatives. Facial liveness innovation avoids spoofing.

Fingerprint scanners—match the one of a kind designs on an individual's fingerprints. A few modern forms of unique mark scanners can indeed evaluate the vascular designs in people's fingers. Unique mark scanners are right now the foremost prevalent biometric innovation for ordinary customers, in spite of their visit mistakes. This ubiquity can be ascribed to iPhones.

Speaker Recognition —also known as voice biometrics, looks at a speaker's discourse designs for the arrangement of particular shapes and sound qualities. A voice-protected gadget ordinarily depends on standardized words to distinguish clients, similar to a watchword.

Eye scanners—include innovations like iris acknowledgment and retina scanners. Iris scanners venture a shinning light towards the eye and explore for special designs within the colored ring around the understudy of the eye. The designs are at that point compared to endorsed data put away in a database. Eye-based confirmation may endure mistakes in case a individual wears glasses or contact focal points.

1.1.5 Token-based authentication

Token-based verification innovations empower clients to enter their accreditations once and get a interesting scrambled string of irregular characters in trade. You'll at that point utilize the token to get to secured frameworks rather than entering your credentials all over once more. The advanced token demonstrates that you just as of now have get to authorization. Utilize token-based verification cases incorporating Tranquil APIs utilized by numerous systems and clients.

1.2 Comparison Table

Authentication Techniques	Method Used	Findings
Password-based authentication	string of letters, numbers, or special characters can be used as Password	Passwords are prone to phishing attacks Difficult to remember many passwords.
Multi-factor authentication	Two or more independent ways to identify a user	Increase the confidence of users by adding multiple layers of security

		MFA may be a good defence against most account hacks. People may misplace their phones or SIM cards, rendering them unable to create a code of authentication
Certificate-based authentication	Digital certificates	Only a certification authority may issue digital certificates to verify public key ownership.
Biometric authentication	based on an individual's unique biological traits	It is simple to compare biological traits. high level of security without causing user friction
Token-based authentication	unique encrypted string of random characters	Instead of entering the credentials again, the token can be used for secured systems.

1.3 eProcurement System

Electronic procurement within the open division is named “electronic open procurement”, “Business to Government” or “B2G”. This handle does not include the buyer sort relationship between an open specialist and its citizens. Nor does it relate to instalment of expenses and charges, by outside associations.

The eProcurement Framework of India empowers the Tenderers to download the Delicate or RFPs of concern office. Plan free of taken a toll and after that yield the offers online through this portal.

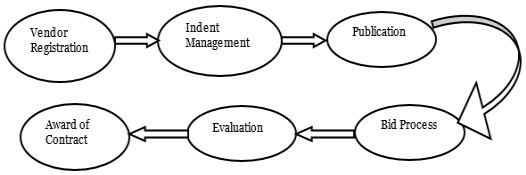

Figure 1: eProcurement Process

In eprocurement system bidders fill bids which is highly confidential detail and government authorities opens the bid and a lot the tender to that bidder. Unless and until proper authentication system of Government authorities or bidders will not exist the transparency of eProcurement system will not be fruitful as per the expectation

2. Conclusion

Confirmation innovation is continuously changing. Businesses need to move past passwords and think of verification as a implies of enhancing client involvement. Verification strategies like biometrics dispose of the ought to remember long and complex passwords. As a result of improved confirmation strategies and advances, attackers will not be able to abuse passwords, and an information breach will be avoided.

3. Acknowledgement

This paper and the inquire about behind it'd not have been conceivable without the extraordinary bolster of my boss, Ani Thomas. Her eagerness, information and demanding consideration to detail have been an motivation and kept motivated me and kept my work headed within the right heading from my beginning of a survey paper.

Refrences

[1] Saru Chandrakar, "Combating Catastrophic Terrorism using Remote Sensing and SARA" in National Conference on Innovations in High Performance Computing and Software Technologies, PP 129, 2008.

[2] Saru Chandrakar, "Detection & Prevention of Terrorist Activities using GIS and Remote Sensing" in International Conference on Futuristic Computer Applications, pp 432-437, 2010.

[3] Saru Chandrakar, "Combating Terrorism using Remote Sensing" in National Conference on

Emerging Trends in Information Technology, 2008.

[4] Saru Chandrakar, "Detection of Explosive using Remote Sensing" in National Conference on Convergence of Technology, 2008.

[5] S. Chandrakar and A. Thomas, "Combating Man-Made Disaster Using Remote Sensing," 2009 Second International Conference on Emerging Trends in Engineering & Technology, 2009, pp. 432-437, doi: 10.1109/ICETET.2009.51. *https://ieeexplore.ieee.org/document/5395058*

[6] Dr. A Vasudeva Reddy Ph.D, MBA, B.Tech(Mech) Assistant Professor, Koneru Lakshmaiah Education Foundation (K L University) K L U Business School Guntur. e-Procurement - Security & Authentication Concerns. *https://aphrdi.ap.gov.in/documents/Trainings@APHRDI/2018/1-jan/eprocurement/e%20Procurement%20-%20Security%20&%20Authentication%20Concerns.pdf*