# Survey on Risk Based Authentication

*[1]Mahesh Kumar Hiremath, [1]Meenakshi, [1]Roshini R, [1]Shravan S K, [2]Syed Akram, [3]Dr Mohammed Misbahuddin.*
*[1]UG Student, Department of Computer Science and Engineering, BMSCE, Bengaluru*
*[2]Assistant Professor, Department of Computer Science and Engineering, BMSCE, Bengaluru*
*[3]Senior Technical Officer, CNIE, CDAC, E-City, Bengaluru,*

***Abstract-*** **Risk Based Authentication system is an authentication system which aims at ways to identify and block fraudulent activities while allowing legitimate users proceed unimpeded and bring balance between usability and security. RBA is an important activity in any web based interactions where a user's behavior is assessed. In this paper various methodologies have been analyzed.**

## I. Introduction

In today's hyper connected world, people are spending more time on internet to complete more of their daily activities such as online banking, e-commerce and social media. However the convenience afforded by the availability of the online world, is not without drawbacks. There has been an unparalleled growth in online fraudulent activities. Trojan, Man in the Middle, Man in the Browser and Phishing attacks are increasing like never before. These threats must be addressed while taking care of the user experience for legitimate users. The demand for improved online identity proofing has gone beyond cybersecurity. Trusted online identity proofing is of major importance to evolving government business operations. This will give a picture of how a risk-based approach to authentication can help organizations maintain balance between user convenience and information security controls necessary to prevent unauthorized access to their information resources and how current systems are exploiting the concept of Risk Based Authentication.

## II. Concept Of RBA

Many existing risk based assessment techniques process the request and classify it as either a low risk or a high risk and demand additional authentication accordingly. Risk can be classified into different levels and suitable additional identity proofs can be asked [1]. More power is provided to the risk based engine in taking decisions so as to alter the risk score of any request and alter the authentication mechanisms that have to be used. The organization making use of the risk based authentication as a security service has the ability to change how the risk based engine takes decisions. A separate database containing historical fraud profiles is maintained as to defend against possible frauds. This method can perform risk authentication

(i) Before the transaction
(ii) During the transaction
(iii) After the transaction.

And when a user fails to authenticate

(i) Authentication with fall back
(ii) Authentication without fall back
(iii) No extra authentication at all

can be carried out. For additional authentication, methods like sending an OTP through SMS/Mail, using shared secrets are suggested.

Authentication in the cloud: A Risk-based Approach [10] gives an overview of the need for user authentication and taking care of identity in cloud. The approach puts forward a cloud based authentication architecture which provides a robust, flexible and scalable authentication system. Risk is categorized into different levels based on user request. The cloud based authentication architecture which is distributed and service provisioning architecture and is supported with SAML2.0 protocol [15].

***Approximate statistics of different concerns related to information security, identity theft and the need for risk based authentication***

According to surveyed statistics by RSA [8]:

- 20% of surveyed population use multifactor authentication, rest use username/password combination.
- Out of 82% of all stolen data, stolen passwords were used in 32% of attacks in 2011.
- 65% allow personal devices to connect to corporate networks.
- 71% of employees use their own mobile devices for business.
- 62% still use password only authentication from mobile devices.

Hence the need to use Risk-Based Authentication with lesser costs, increased security and end user convenience.

***Approach followed***

RSA's fraud detection system [11] analyses an activity to find how legitimate the user is.

Data inputs:

- Set of data facts that identify activity,
- Data from RSA FraudAction Intelligence
- Data from the eFraudNetwork.

Bayesian learning methods are used for making decisions. Intelligent decisions are taken based on analysis of device recognition and user behavior, also receiving a rich feedback from a lot of modules allows RSA Risk Engine to learn when provided with new fraud behaviors.

Risk-Based Authentication provides good flexibility and convenience. RSA Authentication Manager is used for verification of authentication requests and administering of policies for access to enterprise networks. Three things discussed being

1. Manageability with a user dashboard to administer user queries and Self Service Console that allows users to manage their authentication methods.
2. Flexibility allowing using different authenticators hardware or software tokens, on-demand authentication, Risk-based authentication and also a combination. Also considering deployment options, Authentication Manager is offered on a virtual appliance and a hardware appliance.
3. Interoperability with many of the operating system products and network infrastructure.

An overview of RBA working and functionalities as followed in RSA technology [11] which we are also incorporating in our system is provided in brief here. The core of the technology is a risk engine that takes data inputs. It analyses, compares with the user pattern and gives a risk score. If the attempt is found to be risky then further authentication will be followed.

- Device profiling (something that user has) components:
  1. Unique device identification
  2. Device fingerprinting
- Behavior profiling (something the user is or does)
- Risk Assessment and
- Step-Up Authentication forms the system.

The articles on RSA technology gave us a head start. It made clear where the current technology trend lies, what is the scope of the technology that we are trying to touch upon, what are the standards followed under the hood in developing a Risk Based Authentication System.

Risk Based Identity Proofing: A New Approach to Online Identity Verification – by id: analytics [7] white paper gives an overview of the risk based identity proofing, steps taken for isolating non legitimate users from legitimate ones and taking care of high risk occurrences by providing further authentication levels. It gives the fundamental requirements and briefs about how and why it included risk based approach into its system of identity proofing. The technology used includes 3 core capabilities:

1. The ID Network,
2. Personal Topology and
3. Advanced Analytics.

3 step approach of identity evaluation:

1. Determining legitimacy of identity elements using identity resolution technology “Resolve ID”.
2. Assessing identity risk, giving standard identity score “ID Score” by comparing the current identity information with the one present in ID Network.
3. Further authentication measures for higher risk cases. Authentication questions are created by “Certain ID”.

Intelligent Online Risk-Based Authentication using Bayesian Network Model [6] thesis specifies vulnerability in other Risk Based Engine working specifications, they depend on data like IP address, speed of performing transactions by a user. Such kind of data being very vulnerable it questions the robustness and reliability of the existing systems and thus proposes a system that considers key stroke dynamics, mouse dynamics and user site actions in a particular framework. Bayesian network models are proposed which include parameter learning approach and structure learning approach for analyzing the same. The thesis discusses in detail on

- The background knowledge on Bayesian theories
- Technologies used
- Type of data involved
- Feature extraction from data
- Analysis processes
- Noise reduction and discretization.

We could not make use of this system as it requires a greater complexity of software and hardware capabilities moving out from our scope and even after achieving all the complexities the error rate of login attempt by non-legitimate user is still the same.

Most of the risk based authentication methods assess the risk associated with the current authentication request to the typical behavior of a user of the organization.

Say, most of the login requests to an organization come in between 9 am and 7 pm and one particular user sending login requests at 1 am, a typical risk based engine puts the request at 1 am as highly risky(after making a comparison between the current request and all other user's requests). The risk based engine under consideration eliminates such incorrect valuations by comparing a particular user's current login request with his/her previous login requests (user's baseline profile) [2] and thus giving a reasonable result. It uses time windows to keep only the most recent activity for comparison thus saving out on memory space. Mathematical calculations like Standard Deviation, Average Frequency, Proportion, Median, Average etc. are also performed on the user's base lining profile to assess the risk in the current login request.

Another patent, Risk Based authentication duration [3] discloses the idea of assigning the unique session duration for authenticating the user based on the risk associated with that particular user. It is related to authenticating the user based on username, password and key which is valid for a particular amount of time along with his personal credential details for a specific session. If that session

period expires then the user is to provide with another unique session key for further authentication and duration of session key is based on his associated risk. Authenticating the user by the OTP module that is you are given with an OTP id which is valid for a specific amount of time. Once the OTP expires he will be given with the new OTP id for the further authentication but there is risk associated with the generation of OTP according to its associated risk and keeping track of all generation and expiration date for each OTP is difficult and if the user loses his unique OTP then he will be given with more challenging tasks to authenticate himself.

Fraud detection in adaptive authentication system [4] patent discloses the idea of processing an authentication request based on user current data and previous transactions details. The adaptive authentication system which is arranged to perform adaptive authentication operations based on the current user login details and previous transaction details generates authentication request based on the analysis. The system is further arranged to perform an unsupervised machine learning operations on the current details to adjust for the adaptive authentication. While analyzing the user's current login details with the previous details, if we find drastic variation in the major attributes which indicates high level of risk than that particular login details will be stored in fraud database. If the request comes from same attributes then we will block the user. This is how we will perform adaptive authentication of the user. This kind of adaptive authentication helps the user to perform confidential transaction that is low level risk will be processed without much further authentication but the high level risk will be provided with further verification and the adaptive system will be updated with all the user credential to perform adaptive authentication.

AccuTech Systems [9] is the fastest growing trust and investment management software provider in the nation. AccuTech Systems Corp. uses RiskFort, which is the risk-based authentication solution from Arcot Systems. It has proved to be an effective tool in protecting its clients against online fraud and identity theft. AccuTech's clients include trust departments of leading banks, law firms, independent trust companies with wealth management practices, non-profit organizations and governmental agencies that avail to the services of RiskFort.
Accutech Systems adheres to Federal Financial Institutions Examination Council's (FFIEC) guidelines by the usage of Arcot's solution which has the option to add new capabilities, additional layers of security and digital signature without having to change vendors, platforms or technologies. Arcot's RiskFort furnishes strong protection against online fraud in real time by collecting data during the login process to focus on suspicious activity and by formulating a risk score based on the customer's business rules and security protocols. The risk score is used to take a decision on whether the transaction is to be accepted or declined, if a greater degree of authentication is required, or if customer service or network security personnel need to be notified. A unique, secure and easy-to-use access credential, software-only ArcotID is used to enhance online security and business process improvements also adding another factor of authentication security, without changing the familiar username-password login experience of AccuTech's customers or their end users. The customers can use digitally-signed documents to authenticate themselves and to enhance business processes which are legally accepted and non-reputed.

MMORPG massive multiplayer online role playing games [5] is an online game that multiple players can connect and play over the Internet. MMORPG provider exchanges information with each players using adaptive authentication server that facilitates effective adaptive authentication to catch and remove fraudsters. Here analysis of particular user attributes (e.g., the MMORPG player's unique device attributes, ISP address, location, etc.) takes place. Furthermore behavioral analysis of particular player's playing sessions(e. g. a comparison of playing time of day, amount of playing time, purchase habits, the player's unique click stream and other playing activities) are done. Using these, adaptive authentication server will gauge potential risks of fraud (i.e., compute risk scores which assess the risk of fraudsters) and provide input back to provider for taking action. This will protect users from identity theft and misuse of credit information from the player's point of view. This also protects the provider from multiple users using the same account.
Additionally, MMORPG provider communicates with the adaptive authentication server out-of band from the player in order to reform how they operate with the game providers. Further the provider communicates with each player using out-of band communications such as a phone call, an email, a text message etc.
RSA® Adaptive Authentication which is offered by EMC Corporation of Hopkinton is employed for risk-based authentication (RBA) and fraud detection where more than a hundred risk indicators are considered to identify high-risk and suspicious activities. On the other hand, the system also handles financial aspect by with transaction data or defends Web application at login across many verticals. A unique risk score is assigned to each activity, and all players are only challenged when an activity is classified as high-risk or an organizational policy is violated. This boosts security without having to compromise on player convenience.
Disadvantages: A fraudster can infiltrate the MMORPG environment and trick both the players and the provider. For example, a phishing site could steal the player's identifier and password and hijack his/her account thereby manipulating his/her virtual character to lose some or all of the virtual character's virtual items and currency and also to spend actual currency or virtual currency from the hijacked account (i.e., unauthorized micro transactions).

Behavioral Biometrics and Cognitive Security Authentication Comparison Study [12] publication explains authentication system built using 2 concepts: Behavioral biometrics and Cognitive model of authentication system. It shows implementation of a technique called Keyboard Latency for authentication for behavioral biometrics and Association based password authentication for cognitive approach. The keystroke dynamics technology includes taking information of dwell time and time flight giving length of time a key is pressed and time taken to enter successive keys respectively. Enrolment phase collects details to build a model which determines the dynamics of specific user (a reference signature). This signature is used for further authentication to determine risks. If the comparison between the signature stored and current login attempt signature lie within a limit then it is considered low risk else further actions are taken. Considering the cognition model, during registration user gives a range of passwords which are basically the ones that comes to his mind on relating the field in front. This forms the original profile of the user after this comes verification

window where user enters a few of the random passwords that he had given. On submitting a temporary file is created which is compared with the original one and after verification further access is allowed.

OAAM (Oracle Adaptive Access Manager) [13] provides the next-gen of risk based evaluation with real time blocking of frauds. The two core components of OAAM are Adaptive Strong Authenticator that includes range of virtual authenticators and Adaptive Risk Manager. OAAM's Adaptive Strong Authenticator is meant to be an improvement on certain issues handling like data being raw between the point of creation and encryption point, need of a human being to maintain security and protection on data sources and predictable behavior of computing environment. It provides two-factor authentication and encryption of data at the point of entry. Different user interfaces made available here are Question Pad, Quiz Pad, Key Pad, PIN Pad, Slider and Text Pad. Adaptive Risk Manager makes use of a number of ways including one-time use cookies, Flash cookies and other techniques for device identification. It evaluates pre-, post-, and in-session characteristics of each and every transaction assuring fraud detection during transactions. It gives details on different methodologies, techniques, procedures, algorithms, policies followed and other details.

OpenAM, the "all-in-one" open source access management solution for Enterprise and Customer Identity Relationship Management [14], deals with services required for consumer facing identity relationship management and includes Authentication, Entitlements, Federation, Adaptive Authentication, Authorization, Strong Authentication and Web Services Security - as a unified product. The use of common programming interface (REST) makes it easy to call all major OpenAM functions. Session Failover gives the highest level of operational availability to ensure users are always online and connected even across geographically distributed data centers. Deployment becomes easier since it is 100% java based architecture. It's not needed to install any add-on products instead we can turn on any individual services as needed. Adaptive Authentication including device fingerprinting OATH/Soft Token Generator, MSISDN and HOTP (One Time Password) capabilities ensures mobile devices are trusted. For highly sensitive applications and sites, hardware token, biometric device are used as a second factor using mobile phones. Fraud prevention feature uses scoring algorithm that calculates risk score based on an IP address, geolocation, idle time, device fingerprint, etc. and apply to the authentication request such as presenting extra credentials.
OpenAM supports 18+ authentication methods out of the box, along with the potentiality to add new custom methods. Open Identity Gateway Performs HTTP Basic Authentication to the target application and can automatically log users in with password replay.

## III. Conclusion

The Risk Based Authentication System provides security for applications based on the legitimacy of user logging in, allowing legitimate user to proceed unimpeded and block fraudsters.

When a user requests access to an organization, the system collects request-specific information (risk factors). The risk engine, based on the pattern associated with the user and the current attempt details, calculates the deviation associated with the current authentication request then, according to the rules specified by the organization, computes a risk score. Based on the risk score appropriate authentication methods may be carried out.

## IV. References


[1]. Lior Golan, Amir Orad, Naftali Bennett, "System and Method for Risk Based Authentication" Publication Number: US20050097320, May 5, 2005.
[2]. Oded Peer, Yedidya Dotan, Yael Villa, Marcelo Blatt, "Using Baseline Profiles in Adaptive Authentication", Publication Number: US8621586 B1, Dec. 31, 2013.
[3]. Jesper M. Johansson, Darren E. Canavor, David W. Hitchcock, Bothell, "Risk Based Authentication Duration", Publication Number: US8683597, March 25, 2014.
[4]. Yael Villa, Alon Kaufman, Marcelo Blatt,"Fraud Detection in Adaptive Authentication Systems", Publication Number: US8832790, Sept. 9, 2014.
[5]. Yedidya Dotan,"Techniques for authenticating users of massive multiplayer online role playing games using adaptive authentication", Publication Number: US8370389, Feb. 5, 2013.
[6]. "Thesis: Intelligent Online Risk-Based Authentication using Bayesian Network Model" , 2011.
[7]. "Risk-Based Identity Proofing; A New Approach to Online Identity Verification", Feb. 2010.
[8]. www.india.emc.com; resources RSA Authentication Manager, www.emc.com/collateral/
[9]. "CA Advanced Authentication; resources Arcot RiskFort".
[10]. M.T. Dlamini, H.S. Venter, J.H.P. Eloff and Y. Mitha , "Authentication in the Cloud: A Risk-based Approach", 2012.
[11]. "SecurID_Quick_Linksv2"
[12]. "Behavioural Biometrics and Cognitive Security Authentication Comparison Study", "Advanced Computing: An International Journal (ACIJ)", Vol.4, No.6, November 2013.
[13]. "Oracle Adaptive Access Manager. An Oracle White Paper Updated January", 2008.
[14]. "OpenAM –Access Management - All-In-One Solution for Enterprise and Customer Identity Relationship Management by ForgeRock".
[15]. http://en.wikipedia.org/wiki/SAML_2.0.