CONTEXT AWARE SECURE COLLABORATIVE BUSINESS INTELLIGENCE

Veena Jokhakar

Department of ICT, Veer Narmad South Gujarat University, Gujarat, India

ABSTRACT

To enable efficient decision making, professionals need to collaborate with individuals with data being a collected from various sources like distributed clouds for storage, very large databases and social media with authentication and validation is needed for access to relevant roles. Further application of machine learning to deal with unlawful actions. This paper proposes a Context Aware Secure Collaborative Business Intelligence Framework (CASCBF) to address the same. CASCBF is divided into three layers. Multiple sources of data provide different levels of abstraction and granularity of access control to different roles. To control different types of assemblage of data resources from distributed sources and provide right access to users to the edge of the network is a core challenge.

KEYWORDS

Business Intelligence, Attacks, Context Aware, Collaborative BI, Machine Learning.

1. INTRODUCTION

World today has entered an period of time where data is considered as a precious item as money. In today's era data is everywhere and is collected at every second and is being displayed to someone at some location. Business intelligence was described as a environment that is subject oriented, time variant, non-volatile stored in multidimensional storage. This data then can be accessed by report or visualizations or online analytical processing system (OLAP). Enterprise wide data related to each subject of an enterprise with different level granularity is operated on in a multidimensional model used to be stored and visualized known as a data-warehouse also as business intelligence. Figure 1 below shows the classical business intelligence.

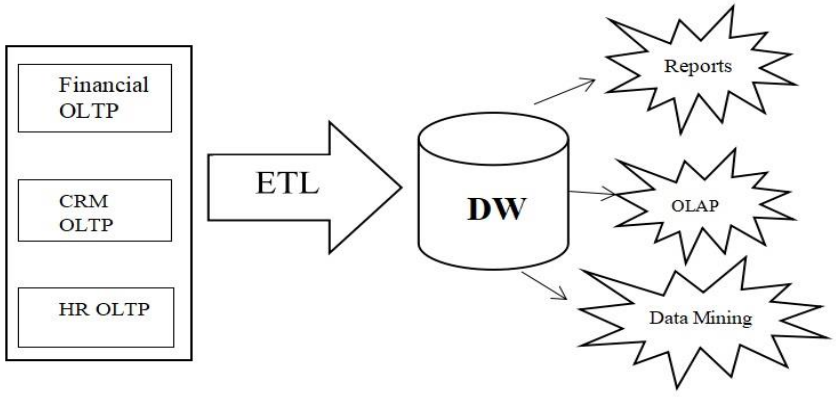

Figure 1. BI Components

Until last few years data warehouse usage had limitation up to its organization only none of its stakeholders, customers used to be a part of it. In last decade business intelligence has grown and extensive work and research activity has been executed to make BI today with Cloud called as Cloud BI example Azure BI from Microsoft where the basic BI remain the same but the data being stored in Cloud. Figure 2 depicted below shows Cloud BI.

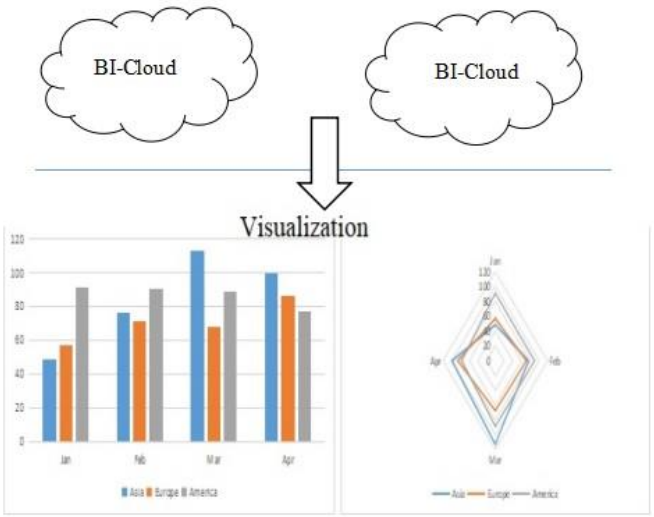

Figure 2. Cloud BI

Shown above Figure 2 portrays the data presentation from Cloud with BI. There are two such clouds shown. In this era of Web 2.0 business intelligence also has to get upgraded to support Web 2.0 architecture this lead to Collaborative Business Intelligence.

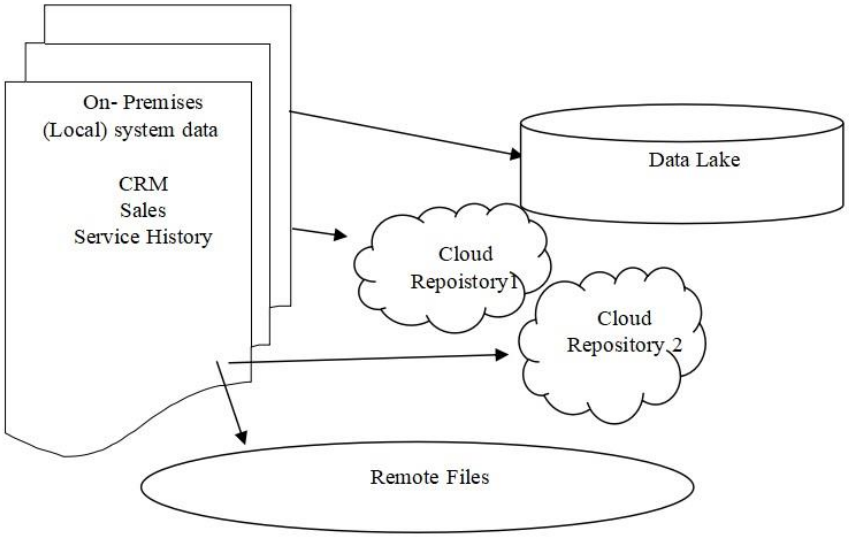

Figure 3. Collaborative BI

The above Figure 3 shows a Collaborative Business Intelligence, where Local enterprise BI connects with Data Lake, that is again a huge repository of raw unprocessed data and various cloud BI as discussed before. And various remote file and database situated remotely.

With the benefits of user interaction and looking at the positive benefits for the enterprise, there exists a danger line too, where the the same company needs to become more cautious and tenacious while operating.

This paper is organized into five sections where Section I gives the introduction, Section II describes various forms of attacks. Section III covers related work in collaborative BI area. Section IV includes proposed framework CASCBF and Section V concludes the paper.

2. FALLACIOUS THREATS - AUTHENTICATION METHODOLOGIES

2.1. Password-based authentication

Authentication is a process of identifying users for accessing data and to display right validated data to the respective users based on their roles. Passwords are the most common methods of authentication which has been exploited widely since last few decades. This is a old- fashioned, cost effective and efficient method to provide access [1]. The two entities (people, computers, services) required to accept they are communicating after authentication and not with intruders [2].

2.2. Multi-factor authentication

Also known as MFA; a two factor authentication also called as 2FA.A smooth user experience mechanism was created by this. For example, if we have swiped our bank card at an ATM and entered a number used as personal identification number. A device will be remembered by MFA approaches, hence for further usage it will be identified easily. [2]

2.3. Certificate-based authentication

The major focus by Mary Thompson and et.al. in [3] is to use the public key infrastructure to provides a secure means of authentication. However additional research and development is needed in advancement in procedure of authorizing. KeyNote, SPKI, and SAML based on X.509 or other key-based identities are the various artifacts or protocols present for authentication but none have been widely adopted. Use of X.509 provides authorization in highly distributed environments, experts have deployed an authorization service based on X.509 which is signed by identified stakeholders. Akenti's goal in the system is to produce authorization system over a secure protocol like transport layer security (TLS) to provide mutual authentication with X.509 certificates between distributed users and resources.

2.4. Biometric authentication

Biometric based authentication is used for convenience along with security. As system is fed with multi facet information, it improves matching execution, increase population extent , disapprove spoofing and alleviate indexing. The need for biometric can be found in a wide range of commercial and military applications [4].

2.5. Token-based authentication

Token based authentication has reduced the risk of stolen authentication factors. When a token is combined with right tokenization system, it becomes a very crucial factor for authorization. Each request is sent to a server accompanied a signed token verified by server for authenticity and then responds to the request in Token based authentication. An open standard (RFC 7519),JSON Web

Token which comprises every detail for securely transmitting information between parties encoded as a JSON object. JWT with small token size allows tokens to be easily transmitted via header attributes, query strings and within the body of a POST request [5].

3. RELATED WORK

Authors of [6] endorse that data-warehousing approaches were meant for having physically materialized data, federative approaches are the ones where the integration happens virtually based on both global schema and P2P approach based data warehouse do not depend on an integrated component data warehouses. They represented a peer-to-peer framework, where peers expose querying functionalities aimed at sharing business information for the decision-making process. The main features of this framework includes decentralization, measurability, and full independence of peers.

Berthold et al. in [7] assert to enable timely and logical decision in BI and focused that ad-hoc analyses is necessary to be performed. The paper aims in realizing a highly scalable and flexible platform for collaborative, ad-hoc BI over large data sets. This can be achieved by developing methodologies, concepts and an infrastructure to enable an information self-service for business users and collaborative decision making within and across organizations over high-volume data sources. In this work, the coarse-grained architecture is conferred and main building blocks that need to be developed were identified.

Umeshwar Dayal and Ravigopal Vennelakanti et al. experts of [8] have explained that enterprises deployed BI technologies to enable strategical decision making. They have described the requirements for collaborative BI and introduced a prototype for collaborative BI platform developed in HP lab. For collaborative BI, they added the ability for collaboration via 3D virtual rooms, visual analytic, and multi-modal interaction technologies for the need of a richer metadata models. To manage complex operations of a large data center, this platform can be used.

Some of the research areas are described which remain unaddressed and can be highlighted through Collaborative BI. Some of them are modeling the experts and associating their knowledge to activities in business and operational processes; capturing meta-data to enable the association of information extracted from heterogeneous structured and unstructured data sources and creation of automated ontologies. Some of the are areas are algorithm development for real-time analytic over event streams, optimization of the end-to-end system to ensure real-time response to event, Recording and analyzing collaboration sessions to discover interaction patterns to improve business and operational processes[8].

Teruel et al. [9] provided a systematic view of BI Application. They analyzed collaborative BI as a new way of making most of out of business processes. There may be loss of information, improper decision as Collaborative BI is executed by exchanging e-mails and documents between the different entities in the business. So, the work proposed a modeling language intended at modeling and educing the goals and information needs of participants of collaborative BI systems.

Metler and et al. in [10] marked that businesses come demanding and comparative. Like it is expected to align along agile business networks by manufacturing organizations in years to come. However they realize that this way of working increases the operating costs and expenses for monitoring and controlling. In this paper the experts have designed a collaborative BI system that may assist companies in optimizing the reliability and highlighted the future research directions.

Hitpass and et al.[11] clearly state the need of transforming business into industry 4. The businesses would be decentralized processes along with decision-making, e-commerce integrated and have real-time control of the automated organizational processes. Collaborative BI is capable of satisfying every point of the need of business. They further ascertain that manual processes have no future and also that business process model will make no sense without e-commerce.

Authors F. Badr and S. Tata [12] ascertain that the leading firms need to collaborate in the economic globalization. Their mechanism offers account informational flows, user preferences and trust. They have represented security in three levels of sensitivity as low, medium and high and have defined rules at each level as white, gray and black. Trust relationships between service providers and customers are established to create communities along with WS-agreement standard extension to describe QoP agreement.

Experts in [13] developed a context aware framework for detecting sensor based threats on smart devices to capture gyroscope, light, etc.. The current smart devices lacks appropriate defense mechanisms for such sensor-based threats. A novel context-aware task oriented sensor-based attack detector for smart devices developed with 6th sense. They had evaluated 6thSense on real devices with 100 different samples and achieved 97% accuracy to detect malicious activities with machine learning. The work included different ML algorithms like Markov Chain, Naive Bayes, and LMT. The 6thSense is highly effective and efficient at detecting sensor-based attacks after empirical evaluation.

Authors of [14] DeBarr and et al. focus on their research work on construction of effective model for spam detection using clustering techniques. The random forest for classification is used for learning spam detection with clustering messages which is efficiently labeling of a representative sample of messages. They have illustrated the results for the 2007 TREC Public Spam Corpus. The area under the Receiver Operating Characteristic (ROC) curve depicted in this paper is competitive with other solutions while requiring much fewer labeled training examples.

Authors in [15][16] projected a hybrid technique for detecting defective coils based on the coiling temperature. They apply association rule mining, classification techniques like KNN, Random forest and SVM and achieve highest accuracy with random forest.

We saw the various works done in the area related to context aware systems, collaborative business intelligence, attack detection and data mining using random forest. Next section focuses on our proposal for new contemporaries of framework.

4. PROPOSED FRAMEWORK

Collaborative BI is the merging or joining of business intelligence software with collaboration tools, including social and Web 2.0 technologies with machine learning along with security to support secure improved data-driven decision making. This framework aims at reducing administrative and computational overheads in secure Collaborative BI systems. A new generation framework of Context-Aware Access Control framework is proposed here which combines the benefits of the Collaborative BI, Web 2.0 and context-aware computing; and ascertain proper access control and security at the edge of the end-devices. This frame work is comprises of three levels as shown in Figure 4.

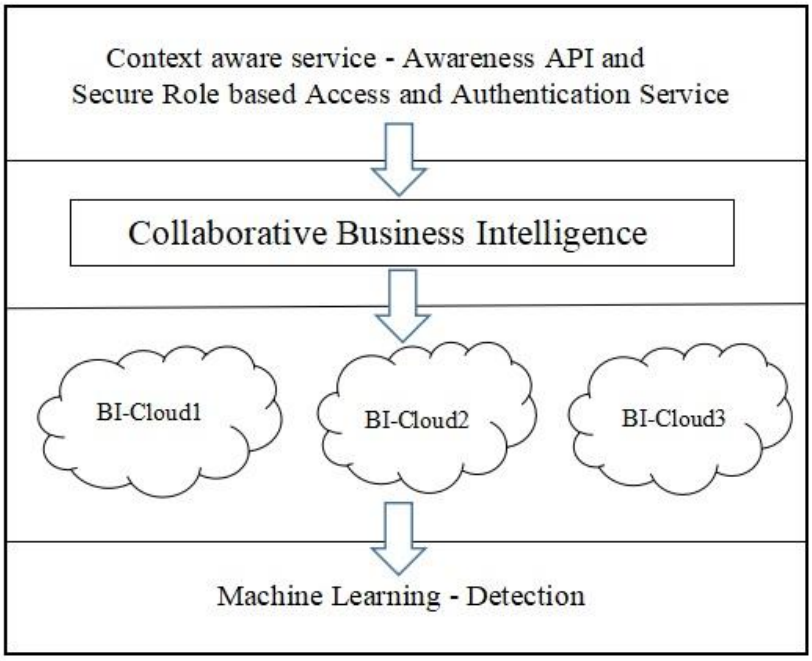

Figure 4. Proposed Framework - Context Aware Secure Collaborative Business Intelligence Framework (CASCBF)

4.1. Level 1 - Secured Context Aware Role Based Access and Authentication Service

Access to systems in today's world is vulnerable to many attacks like unauthorized user access, phishing attacks, installation of viruses, spread of worms etc. In this level of framework user is authenticated based on roles that is aware of the context like geographic location of the access, IP address of the machine, time of access. This can be depicted as shown in the Figure 5.

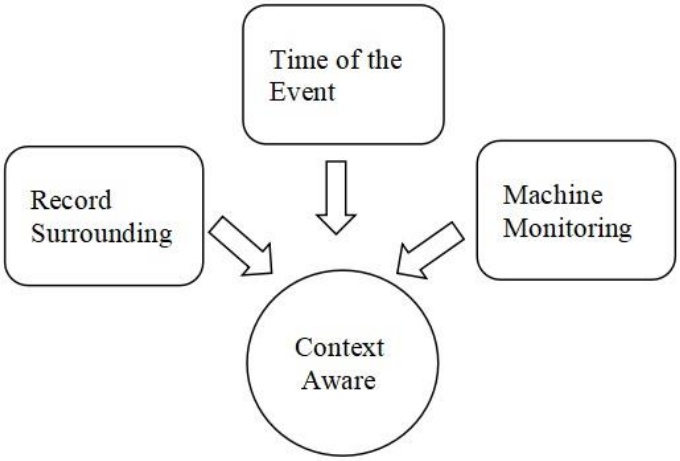

Figure 5. Context aware system aspects

Time of event records the date and time of the access. The record surrounding aspect saves the environment details like geographic location, temperature for check on climate conditions. Machine Monitoring monitors IP address and machine brand. We assert to use the Awareness API, that uses the concept of fences that is taken from geofencing, in which a geographic region,

or geofence is defined, particularly using Fence API, then an application can receive call-backs when a user enters or leaves the geofence region. The Fence API expands on the concept of geofencing to include many other context conditions in addition to geographical proximity. Role based authentication and access provides the allowance to access to the viewable data on the basis of various roles for abstraction of information that is shared at different location along with assigned permissions, which can be addressed using Row Level Security (RLS).

4.2. Level 2 - Collaborative BI with multiple business intelligence systems

Business Intelligence as discussed earlier was meant for storing enterprise level data in tabular or multi-dimensional model. When everything is moving towards cloud due to its advantages, BI also could also be moved to cloud for its advantages. Here we depict the collaborative BI that is to merge traditional BI with collaboration BI tools like Power BI which comes along with functionalities that is social like sharing.

4.3. Level 3 - Machine Learning - Detection

Next phase is Machine Learning layer to detect any abnormal activities like eavesdropping, phishing attacks like masquerading as a trusted entity. By applying AutomatedML (AutoML) data flows with algorithms like decision trees, random forest to detect and predict the possible attacks. We, emphasis more on random forest based on the literature survey, as the RF gives the best performance.

This novel framework in an enterprise can provide secure intelligent means of collaboration in cloud service for further accelerating the business in any area.

5. CONCLUSION

The proposed framework Context Aware Secure Collaborative Business Intelligence Framework (CASCBF) proposes to implement context awareness by creating a service of context aware service using Awareness API and implementing authentication and access by implementing role-based authentication. The next layer collaborative business intelligence that allows to operate on the business data on different granularity levels along with interaction between in various BI, so the decision being taken are more useful and convincing. The third layer of machine learning for detecting various possible attacks using random forest for its explosive way of creating various trees and analysing combination of various technologies makes this framework more powerful concerning aspects of BI, security and context awareness that we want to address.

REFERENCES

[1] Conklin, Wm & Dietrich, Glenn & Walz, Diane. (2004), Password-Based Authentication: A System Perspective.. Proceedings of the Hawaii International Conference on System Sciences. 37. 10.1109/HICSS.2004.1265412.

[2] Syverson, Paul & Cervesato, Iliano. (2001), The Logic of Authentication Protocols. LNCS. 2171. 63-137.

[3] Thompson, Mary & Essiari, Abdelilah & Mudumbai, Srilekha. (2003), Certificate-based Authorization Policy in a PKI Environment. ACM Trans. Inf. Syst. Secur.. 6. 566-588.

[4] Shyam Sunder Yadav, Jitendra Kumar Gothwal , Prof. (Dr.) Ram Singh Maharana Pratap,(2011) Multimodal Biometric Authentication System: Challenges and Solutions, Global Journal of Computer Science and Technology Volume 11 Issue 16 Version 1.0, September 2011 Online ISSN: 0975-4172 & Print ISSN: 0975-4350

[5] Wefel, Sandro & Molitor, Paul. (2012), User Acceptance of Token based Authentication by Single Sign-On. International Journal of Information and Computer Science. 1. 070-077.
[6] Rizzi S., (2012) Collaborative Business Intelligence. In: Aufaure MA., Zimányi E. (eds) Business Intelligence, Lecture Notes in Business Information Processing, vol 96. Springer, Berlin, Heidelberg
[7] Berthold, H., Rösch, P., Zöller, S., Wortmann, F., Carenini, A., Campbell, S., … Strohmaier, F. (2010), An architecture for ad-hoc and collaborative business intelligence. Proceedings of the 1st International Workshop on Data Semantics - DataSem '10
[8] Dayal, U., Vennelakanti, R., Sharma, R., Castellanos, M., Hao, M., & Patel, C. (2008). Collaborative Business Intelligence: Enabling Collaborative Decision Making in Enterprises. Lecture Notes in Computer Science, 8–25
[9] Teruel, M.A., Maté, A., Navarro, E. et al., (2019), The New Era of Business Intelligence Applications: Building from a Collaborative Point of View. Bus Inf Syst Eng 61, 615–634
[10] T. Mettler and D. Raber, (2011), "Developing a collaborative business intelligence system for improving delivery reliability in business networks," 7th International Conference on Concurrent Enterprising, 2011, pp. 1-7.
[11] Hitpass, B., & Astudillo, H. (2019), Industry 4.0 Challenges for Business Process Management and Electronic-Commerce. J. Theor. Appl. Electron. Commer. Res., 14.
[12] Badr, Y., Biennier, F., & Tata, S. (2011), The Integration of Corporate Security Strategies in Collaborative Business Processes. IEEE Transactions on Services Computing, 4(3), 243–254.
[13] Sikder, A. K., Aksu, H., & Uluagac, A. S. (2019), A Context-aware Framework for Detecting Sensor-based Threats on Smart Devices. IEEE Transactions on Mobile Computing, 1–1.
[14] DeBarr, D., & Wechsler, H. (2009). Spam Detection using Clustering, Random Forests, and Active Learning.
[15] Jokhakar V.N., Patel S.V. (2016) Hybrid Associative Classification Model for Mild Steel Defect Analysis. In: Corchado Rodriguez J., Mitra S., Thampi S., El-Alfy ES. (eds) Intelligent Systems Technologies and Applications 2016. ISTA 2016. Advances in Intelligent Systems and Computing, vol 530. Springer, Cham.
[16] S. V. Patel and V. N. Jokhakar, (2016), "A random forest based machine learning approach for mild steel defect diagnosis," 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2016, pp. 1-8.

AUTHOR

Dr. Veena Jokhakar, Ph.D. in Computer Science, having experience of 13 years including industrial and academics, also have 15+ international and national papers to my credit. Her area of interest are Data Science, Datawarehouse, Datamining, Machine Learning and Business Intelligence.