

SYSTEMS AND METHODS FOR DETECTING AND SCORING ANOMALIES

RELATED APPLICATION

This application claims the benefit under 35 U.S.C. § 119 of U.S. Provisional Patent Application No. 62/214,969, filed on September 5, 2015, which is hereby incorporated by reference in its entirety.

This application is filed on the same day as Application Serial No. _____, entitled “SYSTEMS AND METHODS FOR MATCHING AND SCORING SAMENESS,” bearing Attorney Docket No. L0702.70006US00, and Application Serial No. _____, entitled “SYSTEMS AND METHODS FOR DETECTING AND PREVENTING SPOOFING,” bearing Attorney Docket No. L0702.70003US01. Each of these applications is hereby incorporated by reference in its entirety.

BACKGROUND

A large organization with an online presence often receives tens of thousands requests per minute to initiate digital interactions. A security system supporting multiple large organizations may handle millions of digital interactions at the same time, and the total number of digital interactions analyzed by the security system each week may easily exceed one billion.

As organizations increasingly demand real time results, a security system have to analyze a large amount of data and accurately determine whether a digital interaction is legitimate, all within fractions of a second. This presents tremendous technical challenges, especially given the large overall volume of digital interactions handled by the security system.

SUMMARY

According to an aspect of the present disclosure, there is provided a computer-implemented method for analyzing a plurality of first digital interactions observed from a first time period, the method comprising acts of: (A) identifying a plurality of first values of an attribute, each value of the plurality of first values corresponding respectively to a digital interaction of the plurality of first digital interactions observed from the first time period; (B) dividing the plurality of first values into a plurality of buckets; (C) for at least one bucket of the plurality of buckets, determining a count of values from the plurality of first values that fall within the at least one bucket; (D) comparing, by

1a

at least one processor, the count of values from the plurality of first values that fall within the at least

one bucket against historical information regarding the attribute, wherein: the historical information regarding the attribute comprises an expected count for the at least one bucket; the count of values from the plurality of first values that fall within the at least one bucket is compared against the expected count for the at least one bucket; the expected count for the at least one bucket comprises a count of values from a plurality of second values of the attribute that fall within the at least one bucket; each value of the plurality of second values corresponds respectively to a digital interaction of a plurality of second digital interactions; the plurality of second digital interactions were observed from a second time period, the second time period having a same length as the first time period; and the first time period occurs after the second time period; (E) determining whether the attribute is anomalous over the first time period based at least in part on a result of the act (D); and (F) in response to determining that the attribute is anomalous over the first time period, storing, in a profile, information regarding the attribute.

According to an aspect of the present disclosure, there is provided a system for analyzing a plurality of first digital interactions observed from a first time period, the system comprising: at least one processor; and at least one computer-readable storage device having stored thereon executable instructions which, when executed, program the at least one processor to perform a method comprising acts of: (A) identifying a plurality of first values of an attribute, each value of the plurality of first values corresponding respectively to a digital interaction of the plurality of first digital interactions observed from the first time period; (B) dividing the plurality of first values into a plurality of buckets; (C) for at least one bucket of the plurality of buckets, determining a count of values from the plurality of first values that fall within the at least one bucket; (D) comparing the count of values from the plurality of first values that fall within the at least one bucket against historical information regarding the attribute, wherein: the historical information regarding the attribute comprises an expected count for the at least one bucket; the count of values from the plurality of first values that fall within the at least one bucket is compared against the expected count for the at least one bucket; the expected count for the at least one bucket comprises a count of values from a plurality of second values of the attribute that fall within the at least one bucket; each value of the plurality of second values corresponds respectively to a digital interaction of a plurality of second digital interactions; the plurality of second digital interactions were observed from a second time period, the second time period having a same length as the first time period; and the first time period occurs after the second

time period; (E) determining whether the attribute is anomalous over the first time period, based at least in part on a result of the act (D); and (F) in response to determining that the attribute is anomalous over the first time period, storing, in a profile, information regarding the attribute.

According to an aspect of the present disclosure, there is provided a computer-implemented method for analyzing a plurality of digital interactions over a time period, the method comprising acts of: (A) identifying a plurality of values of an attribute; each value of the plurality of values corresponding respectively to a digital interaction of the plurality of digital interactions; (B) dividing the plurality of values into a plurality of first buckets; (C) for at least one bucket of the plurality of first buckets, determining a count of values from the plurality of values that fall within the at least one bucket; (D) comparing, by at least one processor, the count of values from the plurality of values that fall within the at least one bucket against historical information regarding the attribute, wherein: the historical information regarding the attribute comprises an expected count for the at least one bucket; and the count values from the plurality of values that fall within the at least one bucket is compared against the expected count for the at least one bucket; (E) determining whether the attribute is anomalous over the time period, based at least in part on a result of the act (D), comprising: determining if the count of values from the plurality of values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least a selected threshold amount; and in response to determining that the count of values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least the selected threshold amount, dividing the plurality of values into a plurality of second buckets, wherein there are more second buckets than first buckets; and (F) in response to determining that the attribute is anomalous over the time period, storing, in a profile, information regarding the attribute.

According to an aspect of the present disclosure, there is provided a system for analyzing a plurality of digital interactions over a time period, the system comprising: at least one processor; and at least one computer-readable storage device having stored thereon executable instructions which, when executed, program the at least one processor to perform a method comprising acts of: (A) identifying a plurality of values of an attribute, each value of the plurality of values corresponding respectively to a digital interaction of the plurality of digital interactions; (B) dividing the plurality of values into a plurality of first buckets; (C) for at least one bucket of the plurality of first buckets, determining a count of values from the plurality of

values that fall within the at least one bucket; (D) comparing the count of values from the plurality of values that fall within the at least one bucket against historical information regarding the attribute, wherein: the historical information regarding the attribute comprises an expected count for the at least one bucket; and the count of values from the plurality of first values that fall within the at least one bucket is compared against the expected count for the at least one bucket; (E) determining whether the attribute is anomalous over the time period, based at least in part on a result of the act (D), comprising: determining if the count of values from the plurality of values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least a selected threshold amount; and in response to determining that the count of values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least the selected threshold amount, dividing the plurality of values into a plurality of second buckets, wherein there are more second buckets than first buckets; and (F) in response to determining that the attribute is anomalous over the time period, storing, in a profile, information regarding the attribute.

In accordance with some embodiments, a computer-implemented method is provided for analyzing a digital interaction, the method comprising acts of: identifying a plurality of attributes from a profile; for each attribute of the plurality of attributes, determining whether the digital interaction matches the profile with respect to the attribute, comprising: identifying, from the profile, at least one bucket of possible values of the attribute, the at least one bucket being indicative of anomalous behavior; identifying, from the digital interaction, a value of the attribute; and determining whether the value identified from the digital interaction falls into the at least one bucket, wherein the digital interaction is determined to match the profile with respect to the attribute if it is determined that the value identified from the digital interaction falls into the at least one bucket; and determining a penalty score based at least in part on a count of attributes with respect to which the digital interaction matches the profile.

In accordance with some embodiments, a computer-implemented method is provided for analyzing a digital interaction, the method comprising acts of: determining whether the digital interaction is suspicious; in response to determining that the digital interaction is suspicious, deploying a security probe of a first type to collect first data from the digital interaction; analyzing first data collected from the digital interaction by the security probe of the first type to determine if the digital interaction continues to appear suspicious; if the first data collected from

the digital interaction by the security probe of the first type indicates that the digital interaction continues to appear suspicious, deploying a security probe of a second type to collect second data from the digital interaction; and if the first data collected from the digital interaction by the security probe of the first type indicates that the digital interaction no longer appears suspicious, deploying a security probe of a third type to collect third data from the digital interaction.

In accordance with some embodiments, a system is provided, comprising at least one processor and at least one computer-readable storage medium having stored thereon instructions which, when executed, program the at least one processor to perform any of the above methods.

In accordance with some embodiments, at least one computer-readable storage medium having stored thereon instructions which, when executed, program at least one processor to perform any of the above methods.

CLAIMS

1. A computer-implemented method for analyzing a plurality of first digital interactions observed from a first time period, the method comprising acts of:

(A) identifying a plurality of first values of an attribute, each value of the plurality of first values corresponding respectively to a digital interaction of the plurality of first digital interactions observed from the first time period;

(B) dividing the plurality of first values into a plurality of buckets;

(C) for at least one bucket of the plurality of buckets, determining a count of values from the plurality of first values that fall within the at least one bucket;

(D) comparing, by at least one processor, the count of values from the plurality of first values that fall within the at least one bucket against historical information regarding the attribute, wherein:

the historical information regarding the attribute comprises an expected count for the at least one bucket;

the count of values from the plurality of first values that fall within the at least one bucket is compared against the expected count for the at least one bucket;

the expected count for the at least one bucket comprises a count of values from a plurality of second values of the attribute that fall within the at least one bucket;

each value of the plurality of second values corresponds respectively to a digital interaction of a plurality of second digital interactions;

the plurality of second digital interactions were observed from a second time period, the second time period having a same length as the first time period; and the first time period occurs after the second time period;

(E) determining whether the attribute is anomalous over the first time period based at least in part on a result of the act (D); and

(F) in response to determining that the attribute is anomalous over the first time period, storing, in a profile, information regarding the attribute.

2. The method of claim 1, wherein:

each value of the plurality of first values comprises a time measurement between a first point and a second point in the corresponding digital interaction; and

each bucket of the plurality of buckets comprises a range of time measurements.

3. The method of claim 1, wherein:

the act (B) of dividing the plurality of first values into a plurality of buckets comprises applying a hash-modding operation to each value of the plurality of first values; and

each bucket of the plurality of buckets corresponds to a residue of the hash-modding operation.

4. The method of claim 3, further comprising acts of:

(G) recording a plurality of observations with respect to the attribute, each observation of the plurality of observations being recorded from a corresponding digital interaction of the plurality of first digital interactions; and

(H) deriving each value of the plurality of first values based on the observation recorded from the corresponding digital interaction.

5. The method of claim 1, wherein the act (E) comprises:

determining if the count of values from the plurality of first values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least a selected threshold amount, wherein the attribute is determined to be anomalous in response to determining that the count of values from the plurality of first values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least the selected threshold amount.

6. The method of claim 1, further comprising an act of:

(G) dividing the plurality of second values of the attribute into the plurality of buckets.

7. The method of claim 1, wherein the plurality of buckets comprises a plurality of first buckets, and wherein the method further comprises acts of:

(G) determining if the count of values from the plurality of first values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least a selected threshold amount; and

(H) in response to determining that the count of values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least the selected threshold amount, dividing the plurality of values into a plurality of second buckets, wherein there are more second buckets than first buckets.

8. The method of claim 1, further comprising:

(G) selecting a plurality of attributes, the plurality of attributes comprising the attribute, wherein acts (A)-(F) are performed for each attribute of the plurality of attributes.

9. A system for analyzing a plurality of first digital interactions observed from a first time period, the system comprising:

at least one processor; and

at least one computer-readable storage device having stored thereon executable instructions which, when executed, program the at least one processor to perform a method comprising acts of:

(A) identifying a plurality of first values of an attribute, each value of the plurality of first values corresponding respectively to a digital interaction of the plurality of first digital interactions observed from the first time period;

(B) dividing the plurality of first values into a plurality of buckets;

(C) for at least one bucket of the plurality of buckets, determining a count of values from the plurality of first values that fall within the at least one bucket;

(D) comparing the count of values from the plurality of first values that fall within the at least one bucket against historical information regarding the attribute, wherein:

the historical information regarding the attribute comprises an expected count for the at least one bucket;

the count of values from the plurality of first values that fall within the at least one bucket is compared against the expected count for the at least one bucket;

the expected count for the at least one bucket comprises a count of values from a plurality of second values of the attribute that fall within the at least one bucket;

each value of the plurality of second values corresponds respectively to a digital interaction of a plurality of second digital interactions;

the plurality of second digital interactions were observed from a second time period, the second time period having a same length as the first time period; and

the first time period occurs after the second time period;

(E) determining whether the attribute is anomalous over the first time period, based at least in part on a result of the act (D); and

(F) in response to determining that the attribute is anomalous over the first time period, storing, in a profile, information regarding the attribute.

10. The system of claim 9, wherein:

each value of the plurality of first values comprises a time measurement between a first point and a second point in the corresponding digital interaction; and

each bucket of the plurality of buckets comprises a range of time measurements.

11. The system of claim 9, wherein:

the act (B) of dividing the plurality of first values into a plurality of buckets comprises applying a hash-modding operation to each value of the plurality of first values; and

each bucket of the plurality of buckets corresponds to a residue of the hash-modding operation.

12. The system of claim 11, wherein the method further comprises acts of:

(G) recording a plurality of observations with respect to the attribute, each observation of the plurality of observations being recorded from a corresponding digital interaction of the plurality of first digital interactions; and

(H) deriving each value of the plurality of first values based on the observation recorded from the corresponding digital interaction.

13. The system of claim 9, wherein the act (E) comprises:

determining if the count of values from the plurality of first values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least a selected threshold amount, wherein the attribute is determined to be anomalous in response to determining that the count of values from the plurality of first values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least the selected threshold amount.

14. The system of claim 9, wherein the method further comprises an act of:

(G) dividing the plurality of second values of the attribute into the plurality of buckets.

15. The system of 9, wherein the plurality of buckets comprises a plurality of first buckets, and wherein the method further comprises acts of:

(G) determining if the count of values from the plurality of first values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least a selected threshold amount; and

(H) in response to determining that the count of values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least the selected threshold amount, dividing the plurality of values into a plurality of second buckets, wherein there are more second buckets than first buckets.

16. The system of claim 9, wherein the method further comprises an act of:

(G) selecting a plurality of attributes, the plurality of attributes comprising the attribute, wherein acts (A)-(F) are performed for each attribute of the plurality of attributes.

17. A computer-implemented method for analyzing a plurality of digital interactions over a time period, the method comprising acts of:

- (A) identifying a plurality of values of an attribute, each value of the plurality of values corresponding respectively to a digital interaction of the plurality of digital interactions;
- (B) dividing the plurality of values into a plurality of first buckets;
- (C) for at least one bucket of the plurality of first buckets, determining a count of values from the plurality of values that fall within the at least one bucket;
- (D) comparing, by at least one processor, the count of values from the plurality of values that fall within the at least one bucket against historical information regarding the attribute, wherein:
 - the historical information regarding the attribute comprises an expected count for the at least one bucket; and
 - the count values from the plurality of values that fall within the at least one bucket is compared against the expected count for the at least one bucket;
- (E) determining whether the attribute is anomalous over the time period, based at least in part on a result of the act (D), comprising:
 - determining if the count of values from the plurality of values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least a selected threshold amount; and
 - in response to determining that the count of values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least the selected threshold amount, dividing the plurality of values into a plurality of second buckets, wherein there are more second buckets than first buckets; and
- (F) in response to determining that the attribute is anomalous over the time period, storing, in a profile, information regarding the attribute.

18. The method of claim 17, wherein:

- each value of the plurality of values comprises a time measurement between a first point and a second point in the corresponding digital interaction; and
- each bucket of the plurality of first buckets comprises a range of time measurements.

19. The method of claim 17, wherein:

the act (B) of dividing the plurality of values into a plurality of first buckets comprises applying a hash-modding operation to each value of the plurality of values; and
each bucket of the plurality of first buckets corresponds to a residue of the hash-modding operation.

20. The method of claim 17, further comprising the acts of:

(G) recording a plurality of observations with respect to the attribute, each observation of the plurality of observations being recorded from a corresponding digital interaction of the plurality of digital interactions; and

(H) deriving each value of the plurality of values based on the observation recorded from the corresponding digital interaction.

21. The method of claim 17, wherein:

the plurality of digital interactions comprises a plurality of first digital interactions;

the time period comprise a first time period;

the plurality of values comprises a plurality of first values of the attribute;

the method further comprises an act of:

(G) dividing a plurality of second values of the attribute into the plurality of first buckets, each value of the plurality of second values corresponding respectively to a digital interaction of a plurality of second digital interactions;

the expected count for the at least one bucket comprises a count of values from the plurality of second values that fall within the at least one bucket;

the plurality of second digital interactions were observed from a second time period, the second time period having a same length as the first time period; and

the first time period occurs after the second time period.

22. The method of claim 17, further comprising an act of:

(G) selecting a plurality of attributes, the plurality of attributes comprising the attribute, wherein acts (A)-(F) are performed for each attribute of the plurality of attributes.

23. A system for analyzing a plurality of digital interactions over a time period, the system comprising:

at least one processor; and

at least one computer-readable storage device having stored thereon executable instructions which, when executed, program the at least one processor to perform a method comprising acts of:

(A) identifying a plurality of values of an attribute, each value of the plurality of values corresponding respectively to a digital interaction of the plurality of digital interactions;

(B) dividing the plurality of values into a plurality of first buckets;

(C) for at least one bucket of the plurality of first buckets, determining a count of values from the plurality of values that fall within the at least one bucket;

(D) comparing the count of values from the plurality of values that fall within the at least one bucket against historical information regarding the attribute, wherein:

the historical information regarding the attribute comprises an expected count for the at least one bucket; and

the count of values from the plurality of first values that fall within the at least one bucket is compared against the expected count for the at least one bucket;

(E) determining whether the attribute is anomalous over the time period, based at least in part on a result of the act (D), comprising:

determining if the count of values from the plurality of values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least a selected threshold amount; and

in response to determining that the count of values that fall within the at least one bucket exceeds the expected count for the at least one bucket by at least the selected threshold amount, dividing the plurality of values into a plurality of second buckets, wherein there are more second buckets than first buckets; and

(F) in response to determining that the attribute is anomalous over the time period, storing, in a profile, information regarding the attribute.

24. The system of claim 23, wherein:

each value of the plurality of values comprises a time measurement between a first point and a second point in the corresponding digital interaction; and
each bucket of the plurality of first buckets comprises a range of time measurements.

25. The system of claim 23, wherein:

the act (B) of dividing the plurality of values into a plurality of first buckets comprises applying a hash-modding operation to each value of the plurality of values; and
each bucket of the plurality of first buckets corresponds to a residue of the hash-modding operation.

26. The system of claim 23, wherein the method further comprises acts of:

(G) recording a plurality of observations with respect to the attribute, each observation of the plurality of observations being recorded from a corresponding digital interaction of the plurality of digital interactions; and

(H) deriving each value of the plurality of values based on the observation recorded from the corresponding digital interaction.

27. The system of claim 23, wherein:

the plurality of digital interactions comprises a plurality of first digital interactions;

the time period comprises a first time period;

the plurality of values comprises a plurality of first values of the attribute;

the method further comprises an act of:

(G) dividing a plurality of second values of the attribute into the plurality of first buckets, each value of the plurality of second values corresponding respectively to a digital interaction of a plurality of second digital interactions;
the expected count for the at least one bucket comprises a count of values from the plurality of second values that fall within the at least one bucket;

the plurality of second digital interactions were observed from a second time period, the second time period having a same length as the first time period; and
the first time period occurs after the second time period.

28. The system of claim 23, wherein the method further comprises an act of:

(G) selecting a plurality of attributes, the plurality of attributes comprising the attribute, wherein acts (A)-(F) are performed for each attribute of the plurality of attributes.