

computational resources if compared to processing service requests.

Various techniques are known in order to protect processing of service requests against Denial of Service attacks. For example, additional hardware resources may be provided. This, however, is costly and requires additional administrative work. Thus, scalability is limited and, typically, even large-scale hardware resources can be overloaded when an attack is using a plurality of nodes for remitting service requests.

10 A further technique implements a service provider node using cloud-based computational resources. Then, in case of a Denial of Service attack, additional hardware resources can be dynamically provisioned to process all service requests. However, also such a technique is costly, in particular where the additional hardware resources are dynamically allocated.
15 ed. Thresholds for additional hardware resources are often required in order to avoid unexpected costs.

A still further technique requires caching- /proxy providers for minimizing the service requests that have to be processed by the service provider node. However, such an approach has limited efficiency if an attacker requests dynamic content. Dynamic content, typically, has to be processed by the service provider node and cannot be remanded to caching- /proxy providers. Furthermore, sometimes an attacker may have knowledge on the address of the service provider node and may therefore transmit service
20 requests directly to the service provider node, thereby circumnavigating any caching- /proxy providers.
25

WO 2017/145018 A1 discloses a secure method for exchanging entities via a blockchain. Hereby, tokenization techniques and techniques for embedding metadata in a redeem script of a blockchain transaction are included. The method comprises generating a first script, the first script comprising:
30 a first set of metadata associated with a first invitation for the exchange of a first entity by a first user, the first set of metadata comprising an indication of the first entity to be offered for exchange and a first location condition for the exchange, a first user public key
35 (P1A) associated with the first user, wherein the first user public key (P1A) is part of an asymmetric cryptographic pair comprising the first user public key (P1A) and a first user private key (V1A).

XP055444957 discloses a deposit-based rate-limiting approach that requires a deposit before one is able to login, to facilitate denial of service attacks. After paying, the actual authentication procedure
5 take place, i.e, by entering a password. Honest users can expect an immediate refund after the login succeeded. In contrast, malicious attempts are not refunded. Such systems rely on micropayment technologies, such as blockchain-based payment systems that offer the ability to close smart contracts. The system disclosed by this document also can respect concurrent
10 logins:
you can have as many simultaneous login attempts as you like, but each will require another deposit and the price can be adjusted accordingly.

SUMMARY

15 Therefore, in order to provide a reliable, customer-oriented IT service, there is a need to control processing of IT-based service requests. Specifically, there is a need of protecting processing of service request against DoS attacks.

20 It is an object to provide a method for processing of service requests in a controlled and reliable manner.

A method and a service provider node according to the independent claims
25 are provided. Further embodiments are defined in the dependent claims.

According to an embodiment, a method for processing of service requests by a service provider node is disclosed. The method comprises receiving a first service request, which is remitted by a user. The method further
30 comprises receiving first control data indicative of a first financial deposit, which is remitted by the user, wherein the first control data is referenced to at least one service request. The method further comprises processing the received first service request, if the received first control data is referenced to the received first service request. The method
35 further comprises dispensing a third control data indicative of a third financial deposit to the user in response to receiving the first control data and based on an evaluation of a user criterion, wherein the user

criterion includes behaviors of the user, and the method further comprises analyzing the behaviors of the user.

Such an approach is based on the fact that the operational point of time for processing a service request remitted or provided by a user may be controlled using control data related to a financial deposit of the respective service request. The controlled processing of service requests may be admitted when a financial deposit concerning or associated with the respective service request is remitted or executed by the user.

Therefore, the method provides reliable services including protection against fraud including Denial of Service attacks. By requesting a financial deposit before processing a service request, Denial of Service attacks can be effectively mitigated service processing is protected by requiring the financial deposit. Additionally, the dispensing of the third control data enables a refund of financial efforts to a user based on the specifications of the respective user. As an example, a refund of financial efforts of a user may be correlated with the legitimacy of a user for performing the service. Financial incentives may be provided, which may enable not to misapply such a service, wherein on the other hand, legitimated users may be reimbursed and may therefore be able to use the service in a preferably cost-efficient manner.

According to another embodiment, a service provider node adapted to process service requests is disclosed. Hereby, the service provider node comprises a control unit, which is adapted to receive a first service request, which is remitted by a user. The control unit is further adapted to receive a first control data indicative of a first financial deposit, which is remitted by the user, wherein the first control data is referenced to at least one service request. The control unit is further adapted to process the received first service request, if the received first control data is referenced to the received first service request. The control unit is further adapted to dispense a third control data indicative of a third financial deposit to the user in response to receive the first control data and based on an evaluation of a user criterion, wherein the user criterion includes behaviors of the user, and the method further comprises analyzing the behaviors of the user.

Such an approach enables the implementation of preferably simple technical means to perform the method outlined above in a reliable manner.

5 A service request within the meaning of the present disclosure may refer to any user-based inquiry which may intend the provision of a certain service. Such a service may relate to an IT-based service, e.g. a call of a web page sensor control, actuator control, Application Interface (API) access, HTTP GET or POST transactions, etc. The service request may be remitted by a user, i.e. triggered and received from a user.

10 A service provider node within the meaning of the present disclosure may refer to any device, which is adapted to provide IT based services. The service provider node may be adapted to receive service requests and control data indicative of a financial deposit. The service provider node
15 may also be adapted to provide a financial deposit. The service provider node may also be adapted to dispense control data indicative of a financial deposit. The service provider node may also be adapted to dispense a financial deposit. The service preorder node may be implemented by a server.

20 A financial deposit within the meaning of the present disclosure may refer to a transaction of any financial value transferred from a first location to a second location or from a first holder to a second holder. The first location and/or the second location may be accessible to a user.
25 The first location and/or the second location may also be accessible to a service provider.

In an embodiment of the method, the method further comprises storing the received first control data, if the received first control data is not
30 referenced to the received first service request. Hence, it is possible that processing of the service request is delayed. In another embodiment of the method, receiving the first service request is performed after receiving the first control data.

35 Thereby, the method further enables prepayments for services. The method therefore provides for a preferably flexible and user-friendly demand of services with costs.

In another embodiment of the method, receiving the first service request and receiving the first control data is performed simultaneously.

5 Thereby, since these transactions may be performed in a single shot, the method enables a preferably quick and simple processing of services protected by the financial deposits.

10 In another embodiment of the method, the method further comprises receiving a second service request, which is remitted by the user. Hereby, the method further comprises receiving a second control data indicative of a second financial deposit, which is remitted by the user, wherein the second control data is referenced to the at least one service request. This method further comprises processing the received second service request, if the received second control data is referenced to the received second
15 service request. Hereby, receiving the second service request and receiving the second control data is performed simultaneously. Further, receiving the first control and the second control data is enabled by a token dispensed from the service provider node to the user in response to a collective financial transfer performed by the user to the service pro-
20 vider node.

25 Thereby, processing of a plurality of service request may be performed, wherein only a single financial transaction of a user has to be remitted. Thus, the method may reduce efforts dedicated by the user. Therefore, an improved user-friendliness may be achieved.

30 In another embodiment of the method, the user criterion includes at least one of a) at least one service request remitted by the user, b) at least one login attempt of the user and c) financial resource information of the user.

35 Based on a), the behavior of the user concerning his requests for using a service may be analyzed in order to check whether such a user may be legitimated to use the respective service. Hereby, the type of request, the point of time of such a request, variances with respect to the type of request as well as time difference in between two request may be analyzed in order to reliably examine the legitimacy of the respective user for using this service.

Claims

1. A method (100, 200) for processing of service requests
 5 (1) by a service provider node (2), the method (100, 200) comprising:

Receiving (120, 220) a first service request (3),
 which is remitted by a user (4);

Receiving (110, 210) first control data (5) indica-
 10 tive of a first financial deposit (6), which is remitted
 by the user (4), wherein the first control data (5) is
 referenced to at least one service request (1); and

Processing (130, 230) the received first service
 request (3), if the received first control data (5) is
 15 referenced to the received first service request (3);
 wherein the method (100, 200) is characterized by:

Dispensing (270) a third control data (12) indica-
 tive of a third financial deposit (13) to the user (4) in
 response to receiving (110, 210) the first control data
 20 (5) and based on an evaluation of a user criterion,
 wherein the user criterion includes behaviors of
 the user (4), and the method (100, 210) further comprises
 analyzing the behaviors of the user (4).
- 25 2. The method (100, 200) of claim 1, further comprising
 storing (135, 235) the received first control data (5),
 if the received first control data (5) is not referenced
 to the received first service request (3).
- 30 3. The method (100, 200) of any of claims 1 and 2, wherein
 receiving (120, 220) the first service request (3) is
 performed after receiving (110, 210) the first control
 data (5).
- 35 4. The method (100, 200) of any of claims 1 and 2, wherein
 receiving (120, 220) the first service request (3) and re-
 ceiving (110, 210) the first control data (5) is per-
 formed simultaneously.

5. The method (100, 200) of claim 4, further comprising
Receiving (250) a second service request (7), which
is remitted by the user (4);

5 Receiving (240) second control data (8) indicative
of a second financial deposit (9), which is remitted by
the user (4), wherein the second control data (8) is ref-
erenced to the at least one service request (1); and

Processing (260) the received second service re-
10 quest (7), if the received second control data (8) is
referenced to the received second service request (7),

wherein receiving (250) the second service request
(7) and receiving (240) the second control data (8) is
performed simultaneously, and

15 wherein receiving (110, 210, 240) the first control
data (5) and the second control data (8) is enabled by a
token (10) dispensed from the service provider node (2)
to the user (4) in response to a collective financial
transfer (11) performed by the user (4) to the service
20 provider node (2).

6. The method (200) of any of claims 1 to 5, wherein the us-
er criterion includes at least one of a) at least one
service request (1) remitted by the user (4), b) at least
25 one login attempt of the user (4) and c) financial re-
source information of the user (4).

7. The method (200) of any of claims 1 to 6, wherein the
first control data (5) and the third control data (12)
30 are identical.

8. The method (200) of claim 5, further comprising dispens-
ing (280) fourth control data (14) indicative of a fourth
financial deposit (15) to the user (4) in response to re-
35 ceiving (240) the second control data (8) based on an
evaluation of at least one user criterion, wherein dis-
pensing (270, 280) the third control data (12) and the
fourth control data (14) is performed simultaneously.

9. The method (100, 200) of any of the preceding claims,
wherein receiving (120, 220) the first service request
(3) and receiving (110, 210) the first control data (5)
5 is enabled by a data transfer using a distributed data-
base.
10. The method (100, 200) of any of claims 1 to 8, wherein
receiving (120, 220) the first service request (3) and
10 receiving (110, 210) the first control data (5) is ena-
bled by a data transfer using a database (16) based on
distributed ledger technology.
11. The method (100, 200) of claim 10, wherein the use of the
15 database (16) based on distributed ledger technology in-
cludes accessing a Smart Contract service.
12. The method (100, 200) of any of claims 1 to 8, wherein
receiving (120, 220) the first service request (3) and
20 receiving (110, 210) the first control data (5) is ena-
bled by a data transfer using a database (16) based on
Directed Acyclic Graph.
13. A service provider node (2) adapted to process service
25 requests (1) and comprising a control unit (17), which is
adapted to:
 Receive a first service request (3), which is re-
mitted by a user (4);
 Receive a first control data (5) indicative of a
30 first financial deposit (6), which is remitted by the us-
er (4), wherein the first control data (5) is referenced
to at least one service request (1); and
 Process the received first service request (3), if
the received first control data (5) is referenced to the
35 received first service request (3);
 wherein the service provider node (2) is further
characterized in that:

the control unit (17) is further adapted to dispense (270) a third control data (12) indicative of a third financial deposit (13) to the user (4) in response to receive (110, 210) the first control data (5) and
5 based on an evaluation of a user criterion,

wherein the user criterion includes behaviors of the user (4), and the method (100, 210) further comprises analyzing the behaviors of the user (4).

10 14. The service provider node (2) of claim 13, which is adapted to perform the method (100, 200) according to any of claims 2 to 12.