Activity-Based Payments – Alternative (Anonymous) Online Payment Model

Rafał Leszczyna

Received: date / Accepted: date

Abstract Electronic payments are the cornerstone of web-based commerce. A steady decrease in cash usage has been observed, while various digital payment technologies are taking over. They process sensitive personal information raising concerns about its potentially illicit usage. Several payment models that confront this challenge have been proposed. They offer varying levels of anonymity and readiness for adoption. The aim of this study was to broaden the portfolio with a solution that assures the highest level of anonymity and is well applicable. An empirical design research study with prototyping and conceptual research with a proposed construct were employed for this purpose. As a result, the Activity-Based Payment (ABP) model was proposed. It introduces a different mode of completing a payment transaction based on performing specific activities on a web location indicated by the payee. The anonymity properties of the solution, as well as its performance and applicability have been evaluated showing its particular suitability to micropayment and small payment scenarios.

Keywords privacy · e-commerce · micropayments · small payments · applicability · adoption · payment model

1 Introduction

Electronic payments are the primary enabler of web-based commerce. They exhibit many characteristics advantageous to traditional payment systems, including convenience, efficiency, security, privacy or reliability. Consequently, while a decrease in cash usage has been observed, digital technologies are perceived to be a prevalent instrument of consumer payments in the future [1]. Numerous electronic payment systems have been designed since the nineties when electronic commerce gained popularity. They include electronic cash-based systems, account-based systems with credit or debit cards, specialised systems that employ specific techniques for money transfers, and generic systems such as PayPal.

At the same time, the users' awareness of the volume of personal information that is involved in financial transactions is growing. These data can be processed by banks or vendors for purposes other than actual transaction, including direct marketing [2]. Also, websites trace customer spending behaviours to build a competitive advantage [3]. Moreover, the sensitive information may be persistently stored in external databases and serve for deriving even more critical knowledge, including medical conditions, political views or precise geographical location [2]. The anonymity of electronic payments is of great concern [2,4,5,3,6,7] and, together with security, efficiency and flexibility, forms a key requirement for electronic payment systems [8,9].

For these reasons, several electronic payment systems that provide anonymity have been introduced. They take advantage of proxies, virtual accounts, cryptocurrencies, electronic cash and other means, and represent different levels of anonymity, from partial to complete. In the former case, the payer's personal information is concealed from one party (e.g. the merchant) but still revealed to another (e.g. the bank). In the latter, the sensitive data are disguised from all participants. However, regulatory limitations are imposed on their usage.

Gdańsk University of Technology
Narutowicza 11/12, Gdańsk, 80-952, Poland
E-mail: rle@zie.pg.edu.pl

The key objectives of this research were as follows: *RO1*[1]: To design a payment model that complements the existing solutions, broadening the choice of vendors and customers regarding the ways they deliver and acquire products on the e-commerce market. *RO2*: The model should ensure the highest level of anonymity. *RO3*: The model should be applicable, i.e. *suitable to be implemented*.

Pursuing these objectives, a design research study and conceptual research with a proposed construct were employed. To maintain the quality of the contribution and increase its applicability, the relevant recommendations from the Dahlberg et al. study, including general ones, as well as those related to technological research and adoption have been implemented. As a result, the Activity-Based Payment (ABP) model, which introduces an alternative path to completing a payment transaction, has been proposed. It is based on performing specific activities on a web location linked to the payee's service or product. While it ensures the highest level of anonymity of the payer analogous to electronic cash, no tokens or similar cryptographic mechanisms are utilised. Compared to existing approaches, the payment mode may be more suitable for specific applications where payers prefer not to provide any personally-identifiable information or financial data.

The main contributions of the research are:

- An alternative payment model that guarantees the highest level of payer anonymity was proposed.
- The model was implemented in association with an online anonymous e-mail service TAmail (`tamail.org`).
- The anonymity properties of the model were analysed showing the fulfilment of stated requirements.
- System performance was discussed proving the fulfilment of stated requirements.
- The solution's applicability potential was evaluated based on an applicability checklist that helps in verifying whether sufficient effort has been put into increasing the applicability prospects, and a survey that measures participants' perceptions of complexity, usability and acceptance.

The paper is organised as follows. In the next section, the most relevant terminology is introduced. Section 3 presents an analysis of related work based on a systematic literature review method. Section 4 is devoted to the presentation of Activity-Based Payments. Various types of activities can be included in ABP. They are presented in Section 5. Section 6 introduces TApay – a real-world implementation of the ABP model in association with an anonymous e-mailing service. The ABP anonymity level is analysed in Section 7, while the ABP performance is discussed in Section 8. The assessment of the model's applicability potential is presented in Section 9. The paper ends with concluding remarks (Section 10). There, the strength of the proposal as well as its limitations are indicated. The directions for further work are outlined.

[1] RO – Research Objective

2 Terminology

An electronic payment is defined as the transfer of an electronic value from a payer to a payee via an electronic mechanism [10,11,12]. Electronic payments are facilitated by electronic payment systems (EPS) [13,11] that either emulate existing payment frameworks from the non-electronic world or provide new forms of payment transactions [14,11]. According to Shon and Swatman [15], EPS can be broadly categorised into wholesale and retail systems (see Figure 1). Wholesale systems enable corporate-level payment activities, such as automatic salary payments to employees' bank accounts, direct enterprise-to-enterprise payments via banks, or international transfers of funds. Retail systems are dedicated to individual consumers' payment operations [15].

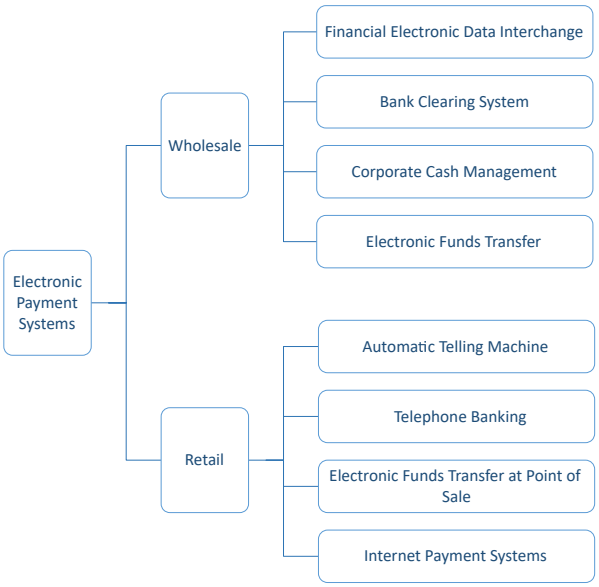

Fig. 1: EPS types according to Shon and Swatman [15]

Another classification was provided by Wayner and followed by Abrazhevich [16,17] who distinguished between token-based and account-based systems. Token-based (or electronic cash-based) systems employ tokens that represent monetary value. They resemble conventional cash and utilise mechanisms such as smart cards or electronic cash. Account-based systems rely on com-

puter network-based communication between banking systems, during which transaction values are transferred and relevant account information – modified. They include credit or debit card systems, specialised systems that employ specific techniques for money transfers (e.g. electronic mail) and generic systems such as PayPal [17]. The classification is illustrated in Figure 2. A similar view was represented by Kim et al. [10] where the five subcategories of cash-based systems and account-based systems include systems based subsequently on electronic cash, prepaid cards, credit cards, debit cards and electronic checks (see Figure 3).

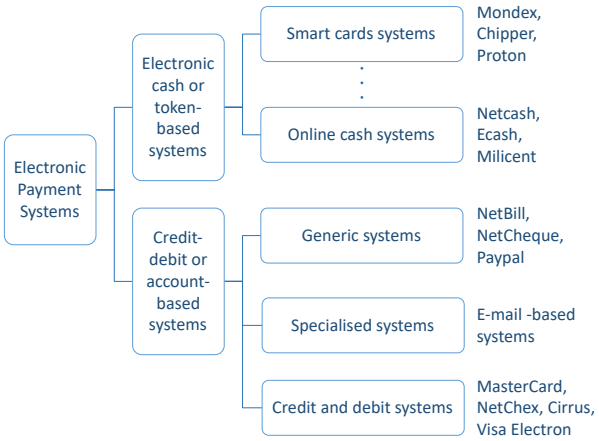

Fig. 2: Classification of EPS according to Wayner and followed by Abrazhevich [16,17]

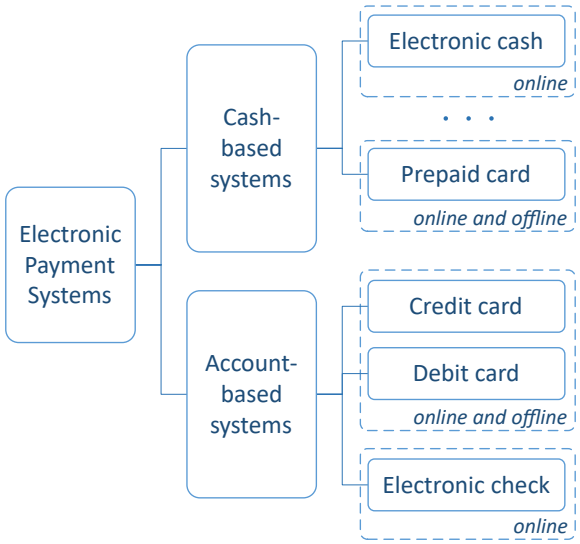

Fig. 3: Kim et al.'s [10] classification of EPS

O'Mahony et al. [18] pointed out mobile payment systems (MPS) as one type of EPS, next to credit card-based systems, electronic checks and account transfers, electronic cash payment systems and micropayment systems. MPS use mobile devices as payment instruments [19,20,21], which, according to Dahlberg et al., is a feature that distinguishes MPS from EPS [22]. Sometimes MPS are perceived as a successor of EPS as far as individual consumers' payment operations are concerned [12]. Because mobile devices and mobile networks are by nature electronic, MPS can be considered as a type of EPS where electronic payment transactions are effected using mobile devices.

3 Related work

Various EPS have been proposed since the nineties when electronic commerce gained popularity [23,18,24]. This includes both academic and commercial endeavours. Many of these proposals have been discontinued during the three-decade evolution of the electronic market [23, 18]. Others, such as PayPal, Apple Pay or Google Wallet strengthened their positions [20,25]. Moreover, new systems and payment scenarios including seamless mobile payments or instant, contactless and open person-to-person payments, have been introduced and broadly adopted [1,26].

This analysis of the relevant work focuses on the solutions that enable anonymous electronic payments, i.e. they protect the anonymity of payers. Aiming at its completeness, a regular literature review process based on Webster et al.'s [27] as well as Kitchenham et al.'s [28] guidelines was implemented (see Figure 4). The analysis embraced both the scientific and patent literature. The ACM Digital Library, Elsevier ScienceDirect, Emerald Insight, EBSCOhost, IEEE Xplore, Web of Science Core Collection and Wiley Online Library databases were used as a source of research papers and books. Keywords including "anonymous", "payment", "link", "website" and related terms (e.g. synonyms) were used in the *literature search* phase when the relevant documents were looked for. The search was directed to documents' titles, abstracts, keywords or other metadata, depending on the capabilities of each particular database. In the literature *selection* stage, irrelevant publications were removed based on simple screening criteria, such as documentation in English, or the presence of a description of an anonymity solution. The *literature analysis* embraced reading the documents partially or entirely to identify the knowledge regarding related anonymity solutions. When identified documents pointed to other related papers, those papers were also subject to the analysis (*backward analysis* [27]).

For patents, a refined search based on extended queries was performed. The Patent Public Search, USPTO Patent Full-Text and Image Database and Google Patents services were employed. Over fifty queries were put into the patent-related databases. A sample query is demonstrated in Listing 1.

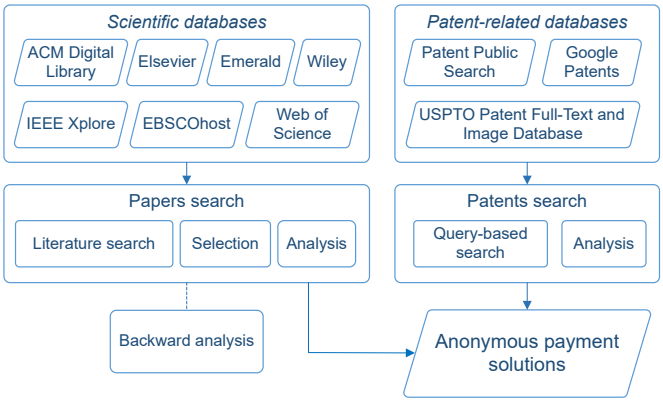

Fig. 4: The main tasks, data sources and results of the related work identification process

Listing 1: Sample query used during the patents search

```
Q01: (G06Q20/00.cpc. OR G06Q20/383.cpc. OR
     G06Q2220/123.cpc. OR H04M2017/248.cpc.
     OR H04M17/306.cpc. OR H04L12/1453.cpc.
     OR H04L12/1464.cpc. OR H04L12/1467.cpc.
     OR H04L2209/56) AND ((anonym* OR hidden
     OR pseudonymous OR incognito OR (protect
      WITH identity) OR (protect WITH
     personal) OR (secure WITH identity) OR (
     secure WITH personal)) WITH20 (link OR
     hyperlink OR url OR address) WITH20 (
     website OR site OR webpage OR page OR
     homepage OR (HTML WITH documents) OR (
     web WITH service) OR (web WITH
     application) OR (web WITH app) OR (web
     WITH process)))
```

3.1 Scientific literature

Chaum's untraceable payments system [29], introduced in 1983, is commonly referred to as the first anonymous electronic payment method [19,25,2,6]. The solution is based on blind signatures and can offer revocable anonymity of a payee or a payer from other participants of a financial transaction. Wang et al. [6,7] proposed another payment scheme that provides *full anonymity*, i.e. the concealment of payer identity from the bank and the payee [5], due to the use of electronic cash. Different levels of anonymity can be achieved depending on the user's choice. The anonymity is revocable in the event of double-spending.

Juang [8] offers complete anonymity as anonymous accounts are established by banks and used for transferring funds to recipients. The accounts need to be funded with electronic cash. A similar solution, but adapted to micropayments, called PlusPay, is specified by Carbunar et al. [30,31]. Also, anonymous accounts are employed to achieve full anonymity, while hash chains help in building micropayment chains to increase payment efficiency. A related, partial-anonymous system, called ORPay was also proposed [31,30].

Scheir et al. [2] carefully considered computations involved in anonymous electronic cash-based payments and the associated performance overhead that rendered many proposals impractical for mobile platforms. They proposed a protocol that is feasible for mobile implementations with all the required security and privacy properties satisfied. This is achieved by performing all uncritical operations on a mobile device and delegating all the sensitive ones to Mobile Trusted Module.

Ni et al. [19] introduced an alternative electronic cash scheme that protects the identities of both payers and payees. Its efficiency was verified analytically and experimentally proving its suitability for mobile phone implementation and mobile payments. Moreover, off-line payment scenarios are possible. Other payment schemes that offer full anonymity due to the use of electronic cash are described in [5,32,33]. A deployed electronic cash system is a prerequisite for each of these frameworks. Also, Martínez-Peláez et al. [34] take advantage of electronic cash to enable anonymous transactions. The proposed scheme is adjusted to micropayments.

Zhang et al. [3] introduced a payment protocol that conceals the purchaser's identity from the merchant and the bank. Symmetrically, the identity of the merchant is protected from the customer and its bank. The protocol assures fair exchange during transactions. Cryptographic mechanisms, including asymmetric cryptography, signatures and nonces are applied for this purpose. The solution requires the modification of the intra-bank transaction system as transaction messages sent between banks are also encrypted according to the proposed scheme.

Since Bitcoin gained popularity, various decentralised payment protocols based on cryptocurrencies have been designed. They provide different levels of privacy, from pseudonymity to full anonymity [19]. Solutions that aim at providing full anonymity include Zerocoin [35], Zerocash [36] and others. An overview of the solutions is provided in [19]. Other Bitcoin-based decentralised anonymous payment systems include [37,38].

Zamanian and Mala [9] introduced protocols that promise full or partial anonymity based on involving mobile network operators instead of financial institutions. Moreover, digital wallets are introduced on the payer's and payee's side. Their state is updated accordingly to each transaction. However, the details of how the wallets are charged with real money are lacking.

Ashrafi and Ng [4] employ asymmetric cryptography and hash functions to hide the customer's identity from the merchant. However, because money transfers are effectuated based on the banking system (credit or debit cards) – the transaction that connects the customer with the merchant is recorded in the banking system. In a similar setting, Isaac and Zeadally [39] apply symmetric cryptography to increase efficiency. Also, a payment gateway is introduced to tackle situations where direct communications between the client and the merchant are not possible.

Chen and Tso [40] framed a concept of near-field communication (NFC)-based mobile payments that take advantage of virtual bank accounts to protect the identity of a user. However, at the initial stage, real personal data are required to establish such an account. Thus, the bank knows the relationship between a virtual account and a real identity. As a result, the identity is fully concealed only from the payee.

As far as the general subject of anonymity is concerned, Pfitzmann and Hansen laid a solid foundation of the anonymity terminology [41] that has been broadly followed in the anonymity domain [42,43]. The main directions of anonymity research concern anonymous communication systems, anonymous data publishing, anonymity metrics, attacks against anonymity, anonymous authentication schemes and others [44,45,46,47,48,49].

3.2 Patents

Regarding the patent literature, McCauley et al. [50] proposed an anonymous payment scheme that takes advantage of anonymising tokens and a payment service system (PSS) acting as an intermediary in all transactions to protect the identity of payees from payers and vice versa. At the initial stage of each transaction, a payee requests that the PSS generates an anonymising token, and upon receipt, presents it to a payer who will use it to finalise the payment. After successful completion, the financial transfer between the accounts of the participants is effectuated by the PSS, which needs to know the relevant account data. Variants of the method adapted to mobile payment scenarios using mobile devices and mobile applications or where the token takes the form of a Quick Response (QR) code are described.

Canard et al. [51,52] patented a method whereby payees are to be paid with electronic cash (in the specification referred to as "anonymous payment means") acquired from an Anonymity Server (SA), through the establishment of anonymous accounts at a Payment Server (SdP). During the cash acquisition, a payer is authenticated by the SA based on their personal data and their private account is debited for an amount corresponding to the amount required by the payer for the electronic cash. Blind signatures are used to provide unlinkability between the payer and the electronic cash. Having the electronic cash, a payer can open an anonymous account at the SdP. The balance will equal the amount of electronic cash. Afterwards, the anonymous funds are intended to be used for payments at merchant sites. However, these steps are not specified in the patent.

3.3 Summary

Chaum's fundamental payment scheme based on blind signatures introduced revocable anonymity of payers and payees during e-commerce transactions [29].

A common approach to anonymous payments is based on introducing intermediate parties (proxies) that hide payer data from the payee in the payment process. However, to finalise payment and assure a real cash flow, payer data need to be provided to financial institutions. For that, they need to be collected and stored in proxies. As a result, only partial anonymity is offered (e.g. from a merchant). Moreover, it can be removed at any moment.

Anonymous accounts or virtual accounts could be a means of fully-anonymous payment if for their opening no personal data were required. Similarly, anonymous virtual credit or debit cards could offer full anonymity, similar to cash, if they could be obtained from a financial institution without providing any personal information. However, in many countries, national regulations require that institutions identify account or card holders. As a result, only partial anonymity can be obtained with such accounts or cards. In practice, they are not available in the offers of banks in such countries.

The customer identification requirement is not strictly enforced on prepaid cards, gift cards or vouchers. This means often such a card or voucher can be obtained from a shop or a service after establishing an account based on fictional data. Also, digital wallets can be interpreted as a form of prepaid card, where the card functions are provided by a computer program. These solutions exhibit a large anonymity potential, especially when acquired or charged by cash at a retailer location. However, their application is limited to a speci-

fied group of payees that recognise and accept them as a means of payment.

As far as cryptocurrencies are concerned, payers' and payees' pseudonyms are stored in the blockchain. In a typical scenario, these pseudonyms are linked to accounts based on verified personal data. Thus, partial anonymity is provided. However, when an account is established without identity verification, using fictional data, and digital coins are acquired anonymously, for instance, by cash via a cryptocurrency automatic teller machine (ATM), by a peer-to-peer platform or by decentralised exchange (DEX) – full anonymity can be achieved. This increases the complexity of using cryptocurrencies. Moreover, it needs to be noted that only a few providers allow the opening of unverified accounts and the fully anonymous mode of currency acquisition.

In this context, electronic cash or e-cash appears to be a promising solution. So far, system complexity and market demands have prevented a wider adoption of its fully anonymous implementation [25,53]. Also, national regulations may prohibit the introduction of anonymous money or limit the obtained level of anonymity. Yet, at the same time, it is worth noting that currently, the introduction of a new version of e-cash is in the preliminary stages in the U.S. [54].

The solution described in the paper aims at complementing the portfolio of the methods by offering an alternative and completely different way of performing anonymous payments while ensuring the highest anonymity level, comparable to e-cash. No personally-identifiable information nor financial data are required for payers. No tokens or similar cryptographic mechanisms are utilised.

The findings of the analysis are summarised in Table 1.

4 Activity-Based Payments

Activity-Based Payments (ABP) is an alternative payment model in which the performance of specific activities to complete a payment is required from a payer. The model assures the anonymity of the payer. Figure 5 illustrates the system infrastructure that enables the implementation of the ABP model. The system comprises one or multiple websites or web services the accessing of which, or accessing and performing of specific activities of which is rewarded by the owner of the website or web service to the party that included a link to the website or web service in their service or product. For clarity of the description, each such website or web service may be referred to as a *rewarding website/web service*. Accessing one or multiple rewarding websites/web services, or accessing one or multiple websites/web services and performing specific activities may be performed by one or multiple payers. It is recommended that the accesses and interactions are performed through an anonymisation proxy such as [55, 56] or I2P [57,58]. In this way, the *untraceability* of the payer, i.e. the state of protection against traffic analysis attacks, is achieved. Traffic analysis involves observing network communications and learning useful information through applying diverse approaches including the correlation of message frequencies, sizes or distinguishing features [43,59,60] (see also Section 7). However, this is an optional component of the ABP system.

Moreover, the system comprises one or multiple services or products provided by a payee. Each of them may have a digital, but also non-digital form. For instance, a physical mailing service enables the physical transfer of items such as letters, postcards and parcels between geographical locations. Its digital equivalent is an e-mail service. Physical products include durable goods such as houses, cars, furniture and computers, and non-durable goods such as food and beverages. Examples of digital products include electronic documents, internet streaming media, website contents and themes, digital videos and graphics, online advertisements, computer applications and games, or virtual goods used within the virtual economies of online games and communities.

Independent of the form, each of the services or products should comprise one or multiple links to one or multiple rewarding websites/web services. For instance, the typical form of a hyperlink, i.e. a text link with an address of a rewarding website/web service, enables the application to both non-digital and digital items. For the former, it is done by writing, painting, printing, or visualising in another way on a non-digital item. For the latter, the link is simply included in digital content. In addition, the system comprises a communication network, e.g. the Internet, that constitutes an intermediary medium that allows a payer to access a rewarding website/web service.

The sequence diagram in Figure 6 presents the interactions involved in an activity-based payment. In the following subsections, each interaction is described in more detail.

4.1 includeLinkToWebsite/WebService

A payee includes one or multiple links to rewarding websites/web services in their service or product. This can be done by visualising in any way (e.g. writing, printing or painting) on any non-digital document associated with a non-digital or digital service, a text link with an address of the rewarding website or web service.

Table 1: Comparison of the proposal and existing approaches for assuring anonymity in electronic payments.

Ref./year	Approach	Advantages	Disadvantages
[29]/1983	Blind signatures	Untraceable payments	Revocable anonymity Potentially complex systems
[3]/2006	Asymmetric cryptography, signatures and nonces	Potential for complete anonymity Fair exchange	Modification of intra-bank transaction system required
[4]/2009	Asymmetric cryptography and hash functions	Customer's identity concealed from the merchant	Partial anonymity
[31]/2009 [9]/2016 [39]/2012 [50]/2021 [51]/2009	Proxies (intermediate parties)	Common approach	Partial and revocable anonymity Potentially complex systems
[8]/2003 [30]/2012 [40]/2016	Anonymous or virtual accounts	Potential for complete anonymity	Partial anonymity in practice Application restricted by law
[10]/2010	Prepaid cards, gift cards, vouchers, digital wallets	Potential for complete anonymity	Application limited to a specified group of payees
[35]/2013 [36]/2014 [37]/2022 [38]/2019	Cryptocurrencies	Potential for complete anonymity (though limited)	Partial anonymity
[6]/2001 [7]/2002 [2]/2015 [19]/2021 [5]/2009 [32]/2009 [33]/2006 [34]/2008	Electronic cash, e-cash	Potential for complete anonymity	Complex Application likely to be restricted by law
This study	Activity Based Payments	Potential for complete anonymity No personally identifiable information nor financial data required No tokens or similar cryptographic mechanisms utilised Primarily applicable to micro and small payments	Complexity dependent on the payment amount Limited applicability to large payments

[1] 'Potential for complete anonymity' means that complete anonymity can be achieved if some additional requirements are satisfied, such as no need to provide any personal data to join the payment model.

The same operation can be performed for the payee's non-digital product, such as a house, a car or furniture. The link may also be introduced into any digital content associated with a digital or non-digital service, or directly included in a digital product.

4.2 followLinkToWebsite/WebService

A payer follows a link to a rewarding website/web service. When a link has the form of a text link with an address of a website and is visualised on a non-digital product or on a non-digital document associated with a non-digital or digital service, following the link may be performed by retyping the address into a web browser on a computing device connected to a communication network and confirming the address to cause the web browser to open the website. For links embedded in digital content, clicking on a representation of the link is a standard way of following a link to cause a web browser to open the website or to cause a web service's client application to access the web service.

4.3 access or accessAndPerformRewardedActivities

Depending on a particular implementation already accessing a rewarding website or web service by a payer may be rewarded by the owner of the rewarding website/web service to the payee. In other scenarios, the payer will need to access a website or web service and perform specific activities that are rewarded by the owner of the website or web service.

4.4 reward

After the payer accessed the website or web service and (when necessary) performed specific activities, the owner of the website or web service rewards the payee. Rewarding can be performed by paying (transferring financial funds). However, in alternative implementations, providing products or services in exchange for including a link to the website or web service in a service or product can be also envisaged.

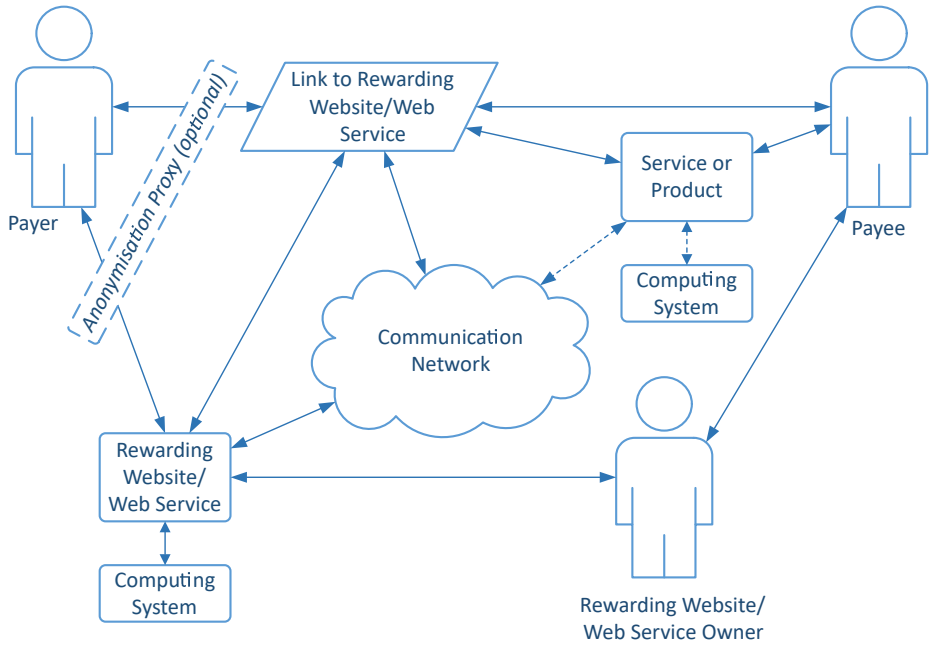

Fig. 5: Main elements of the system infrastructure that enables the implementation of the Activity-Based Payments model

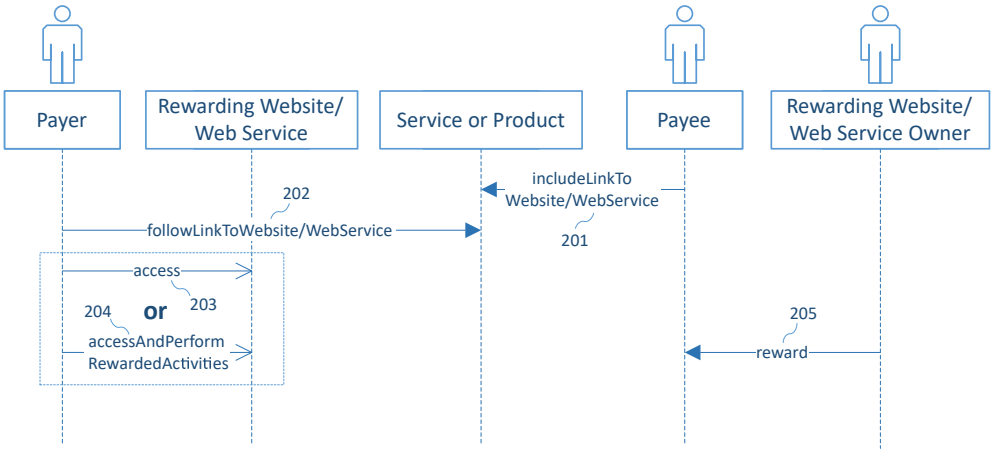

Fig. 6: Sequence diagram of an activity-based payment

5 Payment activities

In a typical scenario, the activities required to effectuate the payment should not require noticeable time or effort from the payer. Otherwise, the complexity of the service and effort expectancy associated with its use would increase negatively affecting the chances of user acceptance and adoption [61,62].

An example of such an undemanding task (probably the most straightforward one) is visiting a website linked from the payee portal and watching advertisements present there. Other examples of straightforward activities are visiting a survey portal and responding to the survey or providing comments on a product, a service or a situation. In more extended implementations, the specific activity requested from a payer may be to perform one or more computations using their computing resources in relation to the content present on the website. For instance, the website may comprise executable code that may be run on the payer's computing device as a specific activity.

Various activities to be performed during the anonymous payment process can be envisaged. They vary in the time of performance and the potential amount of money. Tables 2 – 6 present examples of the activities categorised according to these two factors. The values

are estimated based on general knowledge and [63,64, 65,66,67,68].

Regarding the non-complex activities (see Table 2), multiple programmes that can be used to implement the payment model are available. Affiliate marketing or Pay-Per-Click advertising are two common examples [69,70]. There, usually small amounts of money are granted for each visit to a linked website. Also, linear transaction increases (for instance ± 1 Eurocent), as in traditional payments, are very difficult or even impossible to achieve in the basic scenario. If this feature is required, more complex activities, presented in Tables 3 – 6, need to be implemented in the ABP model.

This includes activities that involve using the technological resources of a payer, for instance, the computational power of their computing device or infrastructure (see Table 3). In this setting, the payer would visit the rewarding website or web service and accept their device to perform computations according to the algorithm or logic of the visited location. In other words, the payment would be based on sharing the computational power of the device. Typically, the more power shared and the longer the time of computation – the larger the amount of payment, starting from very small amounts of money granted for short-time computations [63]. As normally only these are acceptable for payment transactions, the scenario could be applicable primarily to micropayment transactions.

Moreover, human skills can be employed to achieve higher payment amount flexibility. The payer can engage in solving a mathematical, decisional or any other problem presented in the rewarding site or service (see Table 5). Given that the more complex a task, the higher the payback [67] and assuming that a problem-solving performance is linearly dependent on the difficulty of the problem [71], payment amounts can be more flexibly controlled compared to non-complex activities. However, the task completion time is less predictable compared to activities based on technological resources. Among other things, it depends on the difficulty of the task as well as the skills of the solver. At the same time, the amounts of money are higher compared to technological-resource-based activities. Typically, micro and small payments could be achieved in the scheme.

Another type of activity, where human skills are involved, is cyberwork activity (see Table 6). Here, the payer agrees to work during a defined time window to reciprocate for the purchased product or service. These activities provide good control of the payment amount, but the minimum activity times are typically longer. For instance, in a tutoring task, the payer would need to explain specific concepts or how to solve a math problem, which would normally require at least half an hour of involvement.

An activity that provides great/maximum flexibility regarding the amount of money that is transferred and at the same time fits very well the time requirements of a payment process is uploading to a website or web service a digital certificate or a digital item acquired by cash (see Table 4). However, this requires a complex technological infrastructure to verify the validity of the certificate or the value and uniqueness of the digital product.

6 Implementation

The ABP model was implemented in association with the online service TAmail, which enables the exchange of anonymous messages without storing users' personal data. The service, titled TApay, is available at `tamail.org` and allows the sending of e-mails without establishing an account or providing any identification or authentication data. At the same time, responding to e-mails sent in this way is possible, based on temporarily unique message identifiers embedded in them and independent from senders. A sender of an anonymous message needs to record the message identifier in order to provide it to the service any time later to check whether the recipient responded to the message [72].

To ensure the continuity of support of the TAmail service, a funding model based on voluntary micropayments was designed. The continuity of support of a solution is a key factor in its applicability [73]. It results in the solution being maintained, corrected when flows are detected, accompanied with relevant documentation and updated. This, in turn, leads to improved relationships between the users and the suppliers. To prevent reducing the level of anonymity achieved with TAmail, the payments also needed to be anonymous. The ABP model suits well these requirements.

In the implementation, the users of the TAmail service can at any time 'reciprocate' for the possibility of sending and receiving anonymous messages by following the link to a shopping website that participates in an affiliate marketing programme. There, the users need to browse some displayed products. The activity, when recorded by the tracking engine of the affiliate marketing system, results in a small amount of money being attributed to the owner of the TAmail site. Figure 7 presents the TApay subsite of the TAmail portal. The link to the rewarding website has a form of an animated advertisement. A potential limitation of this form of implementation is the risk of the advertisement being disabled by an add-blocker, preventing the payment from being completed.

Table 2: Non-complex activities with low flexibility of payments and small amounts of money transferred

Activity	Performance time	Amounts of money
Watching one or multiple advertisements present on a website	Seconds to minutes	Micro
Responding to a survey, for instance by filling in a questionnaire present on a website	Minutes	Micro, small
Providing a comment on a product, a service, or a situation	Minutes	Micro
Recommending or reviewing one or multiple products or services	Minutes	Micro

Table 3: Resource-consuming activities with increased flexibility of payments and small amounts of money transferred

Activity	Performance time	Amounts of money
Performing one or more computations using the computing resources of a website visitor in relation to the contents present on the website [63]	Minutes – hours	Micro, small
Performing one or more computations using the computing resources of a web service's user according to the logic of the web service	Minutes – hours	Micro, small
Searching the Internet for specific data	Minutes – hours	Micro
Downloading data, including digital products from a website or web service	Seconds – hours	From micro, to potentially large

Table 4: Activities with increased flexibility of payments, including the amounts of money transferred, requiring an extended technological infrastructure

Activity	Performance time	Amounts of money
Uploading valuable data, including digital products to a website or web service	Seconds – hours	From micro, to potentially large
Uploading a digital certificate or a digital item acquired by cash to a website or web service	Seconds	From micro, to large

It needs to be noted that although the implementation introduces voluntary payments accordingly to the funding model, in a typical payment scenario, making a payment is an obligatory step for completing a transaction. This can be illustrated in the example of an anonymous purchase of a product. In this scenario, a purchaser would select a product, confirm the purchase and after that be redirected to the rewarding website. Then, only after confirmation of visiting the site and optionally also performing the necessary activities, would the purchase be completed.

7 Anonymity analysis

In the context of anonymity protection, the following types of attackers are considered during security analyses [59]:

Table 5: Activities with increased flexibility of payments, but difficult-to-estimate completion time (only approximates can be provided)

Activity	Performance time	Amounts of money
Solving a mathematical problem, such as solving an equation or proving a theorem	Minutes – hours	From micro, to small
Solving one or multiple problems specified in the rewarding website	Minutes – hours	From micro, to potentially large
Providing an appropriate decision to a specific decision situation	Minutes – hours	From micro, to potentially large

Table 6: Cyberwork activities

Activity	Performance time	Amounts of money
Playing a character or operating a virtual entity, such as an avatar in a game	Hours	Small
Operating a virtual infrastructure, such as a virtual city or neighbourhood, etc. in a game or similar virtual arrangement	Hours	Small, medium
Tutoring	Hours	Small, medium
Working in cyberspace	Hours	Small, medium

- *Internal* adversaries gain access to a network node such as a server, a host or another computing device participating in communication [60].
- *External* adversaries succeed in accessing one or more network communication links.
- *Single adversaries* have unauthorised access to only one network node [74].
- *K-listening* attackers can observe k network nodes [75].
- *Omnipresent* adversaries are capable of monitoring and analysing the entire network.
- *Passive* adversaries have only read-access type (can only observe) [60].
- *Active* attackers succeed in getting write-access permissions to the analysed network area. As a result, they can modify data and computations [60].
- *Static* attackers choose their attack targets only at the initial stage of an attack [60].
- *Adaptive* adversaries can always change their targets [60].
- *Alliances* of different attackers can be formed.
- Mixed types of attackers (*Hybrids*) such as external-active, k-listening static (*multiple adversary*) and k-listening adaptive adversary (*roving adversary*) can also be distinguished [74].

There are two main attack vectors against anonymity during online activities [43]:

- reading the data content of exchanged communications, and
- performing a *traffic analysis* (TA).

The first class of attacks embraces all activities that involve unauthorised access to the content sent during communication, including the low-level packet data used in network routing. identities, packet sizes, i.e. traffic analysis is based on observing the communications in the available network area, deducing information from communication patterns and packet traffic flow, including the transmission frequency, conversers' identities, packet sizes, etc. to discover the locations and other data of communication participants [76, 43].

Because no personally identifiable data are submitted during transactions, ABP is immune to the higher-level content-reading attacks independent of the attacker type. However, any external adversary that compromised a communication link belonging to the transaction's network route will be capable of reading the

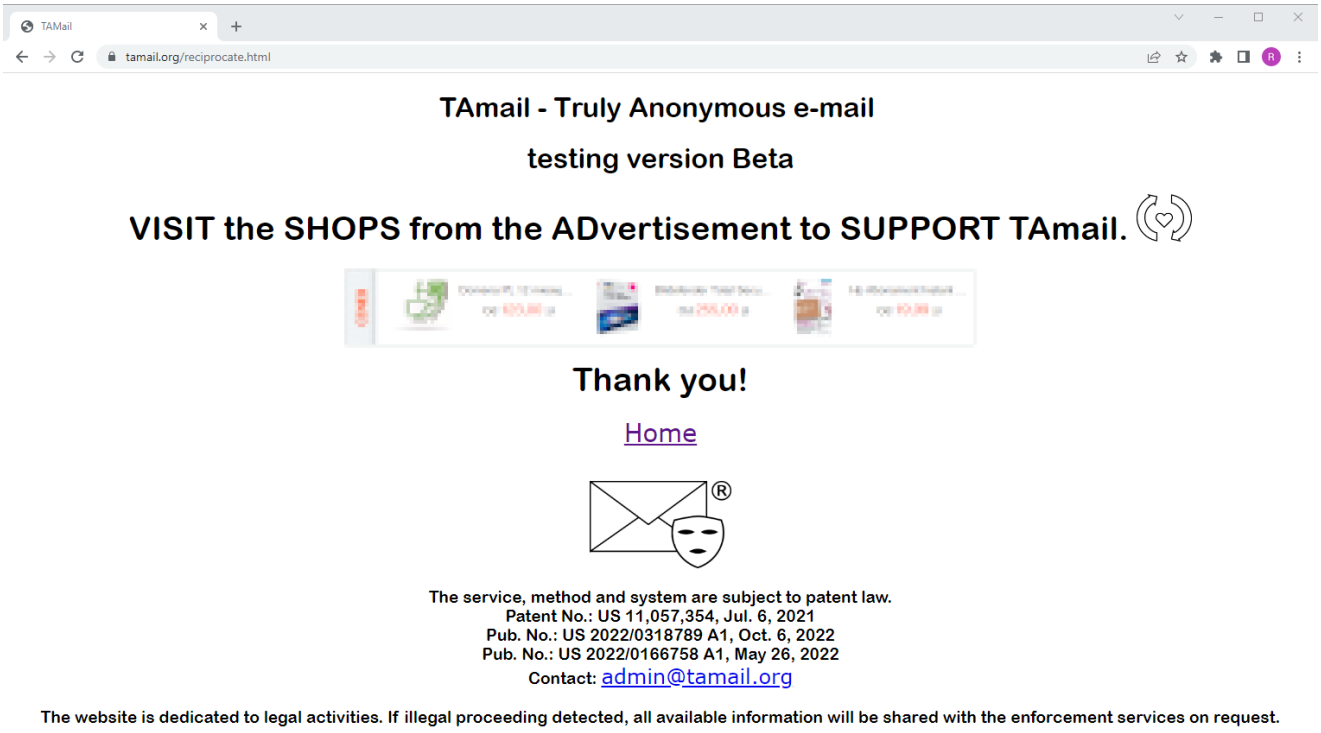

Fig. 7: Activity-Based Payments implementation

packet source and destination identifiers and recognising the source and the target of the communication (e.g. IP addresses). Also, an internal adversary located at any node on the route will be able to read the technical data. If the attackers possess other data that enable connecting the network identifiers with particular entities, e.g. an Internet Protocol (IP) address of an organisation or a user, then the parties involved in the payment can be disclosed to a certain degree. It needs to be noted that obtaining a network identifier of a device belonging to a specific user is very difficult. Moreover, it is not completely certain that the specific user will be using the device at that particular moment. Yet, to increase anonymity protection against internal and external adversaries, anonymising proxies, such as Tor or I2P [56, 58] can be employed. In this case, misleading network identifiers will be visible to the attackers and the identities of the parties participating in the transaction will be protected. It is worth noting that, for instance, the use of Tor is very straightforward. A dedicated web browser needs to be downloaded and launched. Then, accessing websites is identical to a regular browser. All the anonymisation operations are transparent.

For other types of adversaries, including k-listening, omnipresent, passive, active, static and adaptive, as well as alliances and hybrids, analogous reasoning applies. If an attacker gains unauthorised access to a communication link or a network node on the route through which the communication related to the payment transaction is established, the source and destination network identifiers are exposed. Compared to the attacks with single adversaries, protecting against adversaries that captured several network locations (links or nodes) requires more extended configurations of anonymising networks that comprise several proxies.

Summarising, the level of anonymity offered by ABP is equal to e-cash, which offers the highest anonymity level among payment solutions.

8 Performance discussion

In a typical performance analysis scenario, there is a 'fixed' solution, e.g. an algorithm that is subject to time-measuring experiments or time-complexity calculation. For Activity-Based Payments the situation is different in that the (payment) task completion time t_{tc} depends on the type of activity selected for a particular implementation. The t_{tc} values for different sample activities are presented in Section 5, in Tables 2 – 6. They vary between seconds and hours.

Concurrently, except for the tasks that require an extended technological infrastructure, presented in Ta-

ble 4, there is a linear correspondence between t_{tc} and the payment amount p.

$$p \propto t_{tc}$$

The tasks with the shortest t_{tc} enable micropayments. For larger amounts of transfers, transaction times at the level of hours are required.

Consequently, when compared to efficient non-anonymous online payments, such as PayPal or similar, ABP is comparable only for microtransactions. For larger purchases, ABP introduces a substantial overhead. However, when compared to anonymous payment systems, the situation becomes different. ABP offers the highest level of anonymity that is achievable only with e-cash or "mastered" cryptocurrencies, both acquired by cash. For them, while the final transaction alone is instant [77,78], the time dedicated to collecting the anonymous digital money also needs to be considered. The money collection requires a physical visit to an exchange point. Depending on the availability of such a service, the time may vary from minutes to hours. Moreover, the exchanges can vary in frequency. In an optimistic scenario, a large amount of anonymous electronic currency can be taken at the initial stage that will be utilised in multiple anonymous transactions – resulting in the initial time investment being negligible. In a pessimistic one – each transaction may need to be preceded with an exchange, leading to an overhead of minutes to hours. Summarising, it may be assumed that ABP can be an alternative for anonymous micro and small payments.

To illustrate these dependencies, an experiment that aimed at comparing the times of PayPal and ABP transactions was conducted. The experiment was performed in the same system setting for the two operations, i.e. Windows 11 Professional, 12th Gen Intel(R) Core(TM) i3-1215U 1.20 GHz CPU, 16 GB RAM with SSD with Windows Experience Index scores 9, 9.1, 8.1 and 9 for CPU, Disk, Graphics and Memory, subsequently. Using PayPal, the entire operation, from approving the purchase to obtaining payment confirmation took 1 minute and 27 seconds. It consisted of being redirected to the PayPal website, logging into it, obtaining a one-pass code to mobile phone and introducing it into the system. Finally, the card used for payment needed to be selected. A payment associated with the TAmail service (see Section 6) using Activity-Based Payments took 23 seconds. It consisted of clicking on the Voluntary Activity-Based Payments icon (see Figure 17), following the link to a shopping website, being redirected to the website, randomly choosing a product and the shop where it is offered, and finally visiting the shop's website.

The experiment has primarily an illustrative purpose, rather than constituting a precise study according to measurement theory. This is because there are multiple factors, independent of the actual payment system, which influence the payment duration. They are mostly related to the time needed for a system user to perform actions associated with the payment. Various users have different times of signing onto the PayPal system, navigating the site, and reaching their mobile phones to read the one-time passcode and introduce it into the system. Also, there are different network latencies during site redirection and browsing. However, without losing generality, it can be observed that the times are comparable with the precision of 10 seconds. As far as comparing ABP with anonymous payment systems is concerned, practical experiments are prevented by the limited availability of live systems. The prevalence of the frameworks are at the stage of conceptual proposals. Thus, the evaluation was performed based on their literature descriptions.

9 Applicability assessment

This Section presents the results of the evaluation of applicability, i.e. the quality of being applicable [79], or suitability, the ability to be implemented [80]. Applicability's primary constituents are complexity, usability and acceptance [62]. The applicability factors are consistent with mobile payment acceptance factors presented by Dahlberg et al. [23] and Verkijika [81]. The ABP application prospects were assessed based on a dedicated checklist which captures what has been done to increase the potential so far, and a pilot survey of users' impressions on the implemented service.

9.1 Evaluation based on an applicability checklist

To evaluate the progress and completion of design and development activities that aim at increasing the potential of the broad adoption of ABP, the model's applicability features have been evaluated based on a dedicated control list [73,62,82]. The list, with answers indicated, is presented in Table 7.

Regarding question A01, the continuity of ABP is planned to be sustained in connection with the TAmail service [72] (available at `tamail.org`), which is to be funded and maintained for several years by the author of this manuscript. Currently, no training is envisaged for the use of the model as it is expected to be unnecessary, given that making a payment is intuitive. As far as dissemination events associated with the model are concerned, they are also connected to the promotion of

Table 7: Applicability control list. The symbol ☑ depicts a completely addressed control question. ▣ indicates an area that has been partially covered.

A. Continuity of support		
A01. Will your method's continuity be actively maintained with frequent events organised and broad training provided?	Yes ▣	No ☐
A02. Will the method be improved and are new version releases planned?	Yes ☑	No ☐
A03. Have you built a large community of supporters?	Yes ☐	No ☑
A04. Have you developed a funding model that assures the continuity of support?	Yes ☑	No ☐
B. Documentation, tools, target users, method evaluation and completeness		
B01. Have you provided detailed documentation of the method?	Yes ☐	No ☐
B02. Have you developed and shared tools that support the use of the method?	Yes ▣	No ☐
B03. Have you indicated the target users of the method?	Yes ☑	No ☐
B04. Have you tried to minimise the level of skills required to operate the method?	Yes ☑	No ☐
B05. Have you evaluated the effectiveness and efficiency of the method and published information about this?	Yes ☑	No ☐
B06. Have you assured the completeness of results obtained with the method?	Yes ☑	No ☐
C. Complexity, usability, acceptance properties		
C01. Have you tried to reduce the difficulty of understanding of the method?	Yes ☑	No ☐
C02 Have you tried to reduce the difficulty of the description of the method?	Yes ☑	No ☐
C03. Have you tried to reduce the difficulty of the creation of the method?	Yes ☑	No ☐
C04. Have you assured that the method approaches the addressed problem with high precision?	Yes ☑	No ☐
C05. Have you assured that precise results are obtained with the method?	Yes ☑	No ☐
C06. Have you assured that the method comprehensively tackles the entire addressed problem?	Yes ☑	No ☐
C07. Have you evaluated subjective opinions of experts regarding their impressions on using the method?	Yes ▣	No ☐
C08. Have you evaluated users' subjective perceptions of the likelihood that using the method will increase their performance within a specific context?	Yes ☐	No ☑

TAmail. One of the potential directions is attracting the members of the European Energy – Information Sharing & Analysis Centre (EE-ISAC) [83,84,85], where the anonymous sharing of sensitive knowledge on cybersecurity incidents in critical infrastructure is essential.

Improvements in the payment model (question A02) are to be driven by the feedback received from its users. At the current, initial stage of the model design and deployment, a community of supporters has not been established (A03). However, the development of such a community is thoroughly considered in the planning of further exploitation actions, including the involvement of EE-ISAC members, mentioned earlier. The funding model that assures the continuity of support (A04) is currently based on the author's engagement. It embraces several years of support for TAmail and ABP.

As far as ABP documentation is concerned (question B01), it has not been provided due to the straightforwardness and intuitiveness of the model. The documentation will be developed at the request of the users. Among the tools for making Activity-Based Payments (B02), a voluntary anonymous payment system based on non-complex, advertisement-interacting activities has been implemented and deployed so far in connection with the TAmail service. It is described in Section 6. Further developments are currently planned to be focused on the solution, while alternative ABP payment systems based on other activities listed in Tables 2 – 6 will be developed only when necessary, e.g. on request of the users or in association with the development of other anonymous services.

The ABP target users (B03) include all online actors willing to take advantage of anonymous services and anonymously pay for them. Examples include actors taking advantage of anonymous health counselling, anonymous messaging on sensitive issues or anonymous ordering of products or services. The level of skills required to operate the model (B04) has been minimised by design. The use of the model should be straightforward and intuitive, which was partially indicated by the initial evaluation based on a group of students (see the next Subsection). However, currently, the implemented service requires improvements regarding the indication of the payment process and its completion. The effectiveness and efficiency of the method (B05) have been evaluated. The results are presented subsequently in Sections 7 and 8. The model enables the realisation of a complete payment scenario, which satisfies question B06.

The difficulty of understanding, describing and creating the method (questions C01 – C03) has been reduced by design. The model enables anonymous payments with precision, dependent on the activity associated with their realisation (see Tables 2 – 6) (C04-C05). It comprehensively tackles the entire addressed problem of anonymous payments (C06). The subjective opinions of users regarding their impressions on using the method have been evaluated, initially based on the mentioned group of students (C07) (see the next

Subsection). However, users' subjective perceptions of the likelihood that using ABP will increase their performance within a specific context have not been evaluated so far.

The analysis shows that ABP well reflects the majority of determinants related to complexity, usability and acceptance. This constitutes a positive prognosis of the future adoption of the model. The areas of improvement include the development of the community of supporters as well as evaluating the users' and experts' opinions regarding their impressions of using the method and their perceptions of the likelihood that using the method will increase their performance within a specific context. Moreover, subsequent tools that incorporate different payment activities can be developed and deployed in the future.

9.2 Evaluation based on an applicability questionnaire

Additionally, the ABP adoption potential has been assessed based on the applicability questionnaire described in [62]. This was an initial evaluation in which the voluntary payment version of ABP, described in Section 6, was assessed. Thirty-four students completing the last semester of three-year engineering studies of management with a specialisation in management of information technologies participated in the survey. They represented various levels of proficiency in English. Despite the limitations, the survey provided an insightful outcome that will be taken into account in further developments of ABP.

The results show mixed perceptions of the model in the sample group. According to 60% of respondents, the model enables the achievement of its goals, i.e. anonymously paying online for a service or a product (see Figure 8). More than 50% of respondents found the time to complete the task of anonymously paying online for a service or a product acceptable (see Figure 9). Around 45% of participants perceived the task as easy (Figure 10), and 55% of them evaluated the cost and effort of performing the task as lower than expected or about right (see Figures 11 and 12).

At the same time, around 45% of students expressed that the model required too many steps (see Figure 13). This is quite surprising as the number of steps required to complete a payment with ABP is lower than in a typical online payment service such as PayPal (see Table 8).

A similar number of respondents agreed with the statement that the model is overcomplicated (see Figure 14). As a consequence, almost half of those surveyed were not satisfied with ABP (Figure 15) and perceived

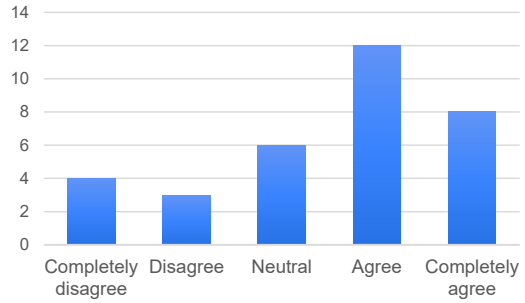

Fig. 8: Responses to question 1 – The model enables its goals to be achieved, i.e. anonymously paying online for a service or a product.

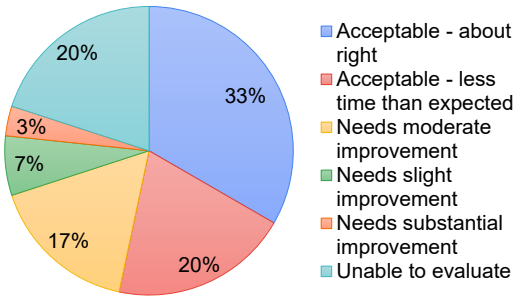

Fig. 9: Responses to question 16 – Time to complete the task.

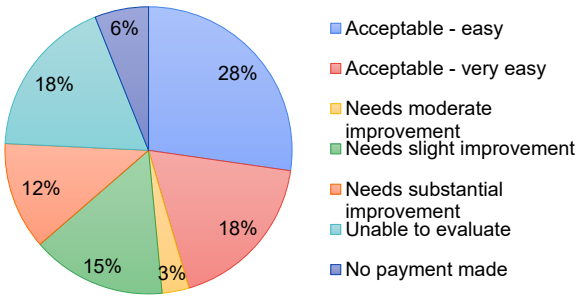

Fig. 10: Responses to question 17 – Ease of performing the task.

that the model did not have all the expected functions and capabilities (16).

The comments regarding the missing function revealed that ten out of the thirty participants (around 30%) had a problem with understanding that performing the advertisement-watching activity is a way to complete payment. This might be the reason for the outcome of questions Q2 – Q5 connected to the voluntary mode of payments which to some participants might be misleading. For instance, the iconic representation of the payment (reciprocation for the use of the service, see Figure 17) may not be intuitively associated with payments. Also, the result could be partially attributed to the language of the ABP implementa-

Table 8: The number of steps required to complete a payment with a typical online payment service and ABP

No.	ABP	Typical online payment service
1.	Go to the linked rewarding website	Go to the financial agent site
2.	Go to a website indicated in the rewarding website	Sign in and authenticate
3.	Return to the site of origin	Confirm the payment
4.		Authenticate the payment (e.g. using a passcode received by SMS)
5.		Return to the site of origin

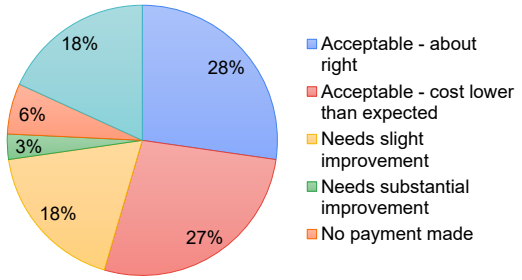

Fig. 11: Responses to question 18 – Cost of performing the task.

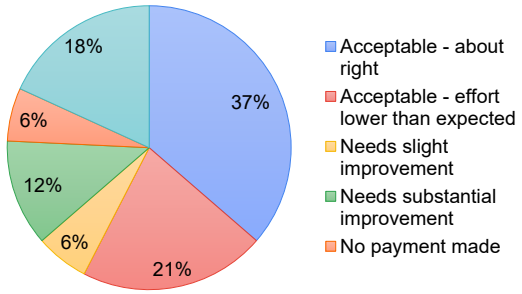

Fig. 12: Responses to question 19 – Effort to perform the task.

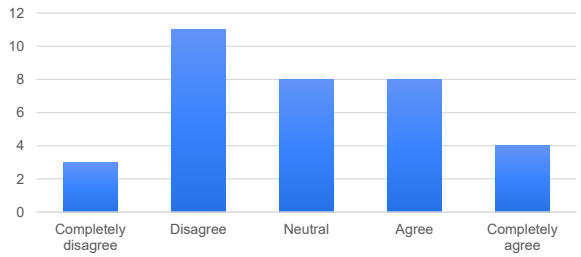

Fig. 13: Responses to question 2 – The model requires too many steps to pay for a service or a product.

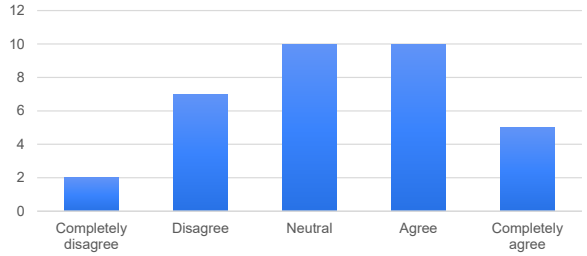

Fig. 14: Responses to question 3 – The model is too complicated.

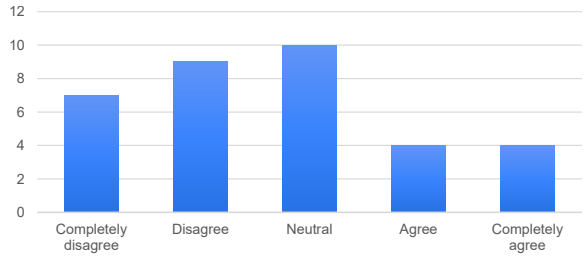

Fig. 15: Responses to question 4 – "Overall, I am satisfied with the model."

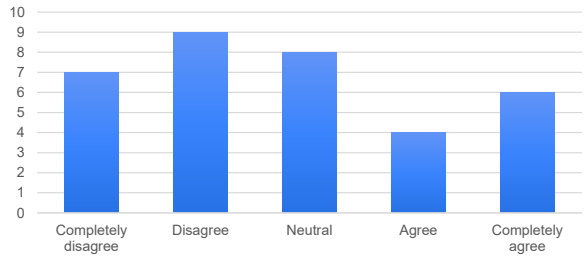

Fig. 16: Responses to question 5 – "The model has all the functions and capabilities I expect it to have."

tion (English) corresponding with the potentially insufficient linguistic proficiencies of some participants. Nevertheless, the results are valuable by pointing out the areas for further improvement.

Other constructive comments included the lack of an indication that the rewarding site was entered and the payment process was successful. Moreover, one respondent requested a "more professional graphic design". These comments will be considered during further works; however, the straightforward, simplistic design of the service was chosen deliberately to assure high efficiency of the system independent of the technological platform on which it is run. At the moment, only around 25% of the sample group would use ABP more frequently and recommend it to others (see Figures 18 – 19).

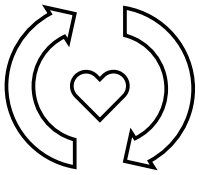

Fig. 17: Voluntary Activity-Based Payments icon

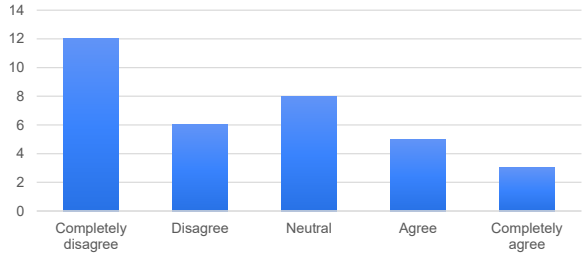

Fig. 18: Responses to question 7 – "I would like to use the model more frequently."

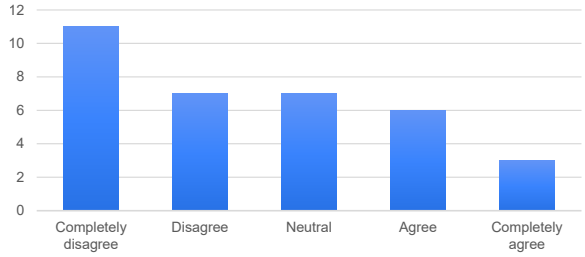

Fig. 19: Responses to question 8 – "I would recommend the model for being used by others."

The results are quite critical, which may be partially attributed to the limitations of the initial evaluation indicated earlier. The main conclusions assume a more visible indication of the payment process and its completion as well as repeating the evaluation with larger and more diverse samples.

10 Conclusions

The paper presented an alternative online payment model – Activity-Based Payments (ABP) – that can find its application in the areas where the payer's anonymity is of primary concern. The model does not require any personal data or financial information from payers. At the same time, it does not require cryptographic mechanisms, which has a positive impact on resource consumption and enables application on platforms with limited computational power. It introduces a new way of completing a payment that is based on performing specific activities on a web location indicated by the payee. The analysis of the ABP performance revealed that for micropayments and small payments its efficiency is comparable to common online payment systems. At the same time, making activity-based payments of larger amounts introduces an overhead that may be unacceptable to users. The ABP adoption potential was evaluated based on a dedicated checklist and a pilot survey. The former confirmed a major effort devoted to increasing the chances of adoption. The latter provided a critical insight that will be addressed in further developments. Consequently, the key objectives of the research have been achieved. The proposals' strengths and limitations as well as future work are summarised in Table 9.

Statements and declarations

The author declares that he has no known competing financial interests or personal relationships that could appear to influence the work described in this paper.

Data availability statement

The pilot implementation of the TApay payment model based on following advertisements is available publicly at `tamail.org`. Other research data generated during the current study are available from the corresponding author upon reasonable request.

References

1. Kantar Public: Study on new digital payment methods. Technical report, European Central Bank (2022)
2. Scheir, M., Balasch, J., Rial, A., Preneel, B., Verbauwhede, I.: Anonymous split e-cash—toward mobile anonymous payments. ACM Trans. Embed. Comput. Syst. **14**(4) (2015). https://doi.org/10.1145/2783439
3. Zhang, Q., Markantonakis, K., Mayes, K.: A practical fair-exchange e-payment protocol for anonymous purchase and physical delivery. In *IEEE International Conference on Computer Systems and Applications, 2006.*, pp. 851–858. 2006 (2006). https://doi.org/10.1109/AICCSA.2006.205188
4. Ashrafi, M.Z., Ng, S.K.: Privacy-preserving e-payments using one-time payment details. Computer Standards & Interfaces **31**(2), 321 (2009). https://doi.org/10.1016/j.csi.2008.04.001
5. Bakhtiari, S., Baraani, A., Khayyambashi, M.R.: Mobicash: A new anonymous mobile payment system implemented by elliptic curve cryptography. In *2009 WRI World Congress on Computer Science and Information Engineering*, vol. 3, pp. 286–290. 2009 (2009). https://doi.org/10.1109/CSIE.2009.939
6. Wang, H., Cao, J., Zhang, Y.: A consumer scalable anonymity payment scheme with role based access control. In *Proceedings of the Second International Conference on Web Information Systems Engineering*, vol. 1, pp. 53–62 vol.1. 2001 (2001). https://doi.org/10.1109/WISE.2001.996466

Table 9: Strengths, limitations and further work on Activity-Based Payments.

Strengths	Limitations	Further work
A new mode of completing a payment transaction	Complexity dependent on the payment amount	Development of the community of supporters, starting from the liaison with EE-ISAC
Broadening the portfolio of anonymous e-payment methods with an alternative	Limited applicability to large payments	Evaluation of users' and experts' opinions regarding their impressions of using the method and their perceptions of the likelihood that using the method will increase their performance within a specific context
Suitable for applications where payers are privacy-concerned	Linear transaction increases (for instance ± 1 Eurocent) difficult to be achieved with basic activities	
The highest level of anonymity of the payer analogous to the electronic cash assured	Assessment of mobile payment adoption (applicability) chances based on a small sample	Implementation of other payment modes and activities when driven by the market need
No tokens or similar cryptographic mechanisms utilised	Applicability evaluation focused on a voluntary payment mode	Including more visible indications of the payment process and its completion in the ABP system Graphical User Interface
Flexibility in the selection of payment activity from a large portfolio	Risk of advertisement-based payment activities being disabled by an add-blocker	Repeating applicability assessments with larger and more diverse samples
Increased adoption potential confirmed by an applicability checklist-based evaluation		Performing an applicability evaluation of other payment modes
Dahlberg et al.'s recommendations incorporated to ensure high quality		

7. Wang, H., Cao, J.: Building a consumer scalable anonymity payment protocol for internet purchases. In *Proceedings Twelfth International Workshop on Research Issues in Data Engineering: Engineering E-Commerce/E-Business Systems RIDE-2EC 2002*, pp. 159–168. 2002 (2002). https://doi.org/10.1109/RIDE.2002.995110
8. Juang, W.S.: A practical anonymous payment scheme for electronic commerce. Computers & Mathematics with Applications **46**(12), 1787 (2003). https://doi.org/10.1016/S0898-1221(03)90237-9
9. Zamanian, F., Mala, H.: A new anonymous unlinkable mobile payment protocol. In *2016 6th International Conference on Computer and Knowledge Engineering (ICCKE)*, pp. 117–122. 2016 (2016). https://doi.org/10.1109/ICCKE.2016.7802126
10. Kim, C., Tao, W., Shin, N., Kim, K.S.: An empirical study of customers' perceptions of security and trust in e-payment systems. Electronic Commerce Research and Applications **9**(1), 84 (2010). https://doi.org/10.1016/j.elerap.2009.04.014. Special Issue: Social Networks and Web 2.0
11. Oney, E., Guven, G.O., Rizvi, W.H.: The determinants of electronic payment systems usage from consumers' perspective. Economic Research-Ekonomska Istraživanja **30**(1), 394 (2017). https://doi.org/10.1080/1331677X.2017.1305791
12. Gonzalez, D.: Chapter 8 - currency and campaigns. In *Managing Online Risk*, ed. by Gonzalez, D., pp. 185–211. Butterworth-Heinemann, Boston, 2015 (2015). https://doi.org/10.1016/B978-0-12-420055-5.00008-6
13. Lim, B., Lee, H., Kurnia, S.: Exploring the reasons for a failure of electronic payment systems: A case study of an australian company. Journal of Research and Practice in Information Technology **39**(4), 231 (2007)
14. Tsiakis, T., Sthephanides, G.: The concept of security and trust in electronic payments. Computers & Security **24**(1), 10 (2005). https://doi.org/10.1016/j.cose.2004.11.001
15. Shon, T., Swatman, P.M.: Identifying effectiveness criteria for internet payment systems. Internet Research **8**(3), 202 (1998). https://doi.org/10.1108/10662249810217759
16. Wayner, P.: Digital Cash (2nd Ed.): Commerce on the Net. Academic Press Professional, Inc., USA, 1997 (1997)
17. Abrazhevich, D.: Classification and characteristics of electronic payment systems. In *Electronic Commerce and Web Technologies*, ed. by Bauknecht, K., Madria, S.K., Pernul, G., pp. 81–90. Springer Berlin Heidelberg, Berlin, Heidelberg, 2001 (2001)
18. O'Mahony, D., Pierce, M., Tewari, H.: Electronic Payment Systems for E-Commerce, Second Edition. Artech, 2001 (2001)
19. Ni, J., Au, M.H., Wu, W., Luo, X., Lin, X., Shen, X.S.: Dual-anonymous off-line electronic cash for mobile payment. IEEE Transactions on Mobile Computing pp. 1–1 (2021). https://doi.org/10.1109/TMC.2021.3135301
20. Liu, W., Wang, X., Peng, W.: State of the art: Secure mobile payment. IEEE Access **8**, 13898 (2020). https://doi.org/10.1109/ACCESS.2019.2963480
21. Tso, R.: Untraceable and anonymous mobile payment scheme based on near field communication. Symmetry **10**(12) (2018). https://doi.org/10.3390/sym10120685
22. Dahlberg, T., Guo, J., Ondrus, J.: A critical review of mobile payment research. Electronic Commerce Research and Applications **14**(5), 265 (2015). https://doi.org/10.1016/j.elerap.2015.07.006. Contemporary Research on Payments and Cards in the Global Fintech Revolution
23. Dahlberg, T., Mallat, N., Ondrus, J., Zmijewska, A.: Past, present and future of mobile payments research: A literature review. Electronic Commerce Research and Applications **7**(2), 165 (2008). https://doi.org/10.1016/j.elerap.2007.02.001. Special Section: Research Advances for the Mobile Payments Arena
24. Carat, G.: epayment systems database - trends and analysis. Technical report EUR 20264 EN, Electronic Payment Systems Observatory (ePSO), Institute for Prospective Technological Studies Directorate General Joint Research Centre European Commission, Seville, Spain (2002)
25. Braeken, A.: An improved e-payment system and its extension to a payment system for visually impaired and blind people with user anonymity. Wireless Personal Communications **96**(1), 563 (2017). https://doi.org/10.1007/s11277-017-4184-5
26. EMPSA european mobile payment systems association. `https://empsa.org/`. Accessed 10 January 2024
27. Webster, J., Watson, R.T.: Analyzing the past to prepare for the future: writing a literature review. MIS Quarterly **26**(2), xiii (2002)
28. Kitchenham, B., Brereton, P.: A systematic review of systematic review process research in software engineering. Information and Software Technology **55**(12), 2049 (2013). https://doi.org/10.1016/j.infsof.2013.07.010

29. Chaum, D.: Blind signatures for untraceable payments. In *Advances in Cryptology*, ed. by Chaum, D., Rivest, R.L., Sherman, A.T., pp. 199–203. Springer US, Boston, MA, 1983 (1983)
30. Carbunar, B., Chen, Y., Sion, R.: Tipping pennies? privately practical anonymous micropayments. IEEE Transactions on Information Forensics and Security **7**(5), 1628 (2012). https://doi.org/10.1109/TIFS.2012.2204982
31. Chen, Y., Sion, R., Carbunar, B.: Xpay: Practical anonymous payments for tor routing and other networked services. In *Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society*, WPES '09, p. 41–50. Association for Computing Machinery, New York, NY, USA, 2009 (2009). https://doi.org/10.1145/1655188.1655195
32. Popescu, C.: An anonymous mobile payment system based on bilinear pairings. Informatica **20**(4), 579 (2009). https://doi.org/10.15388/Informatica.2009.267
33. Wei, K., Smith, A., Chen, Y.F., Vo, B.: Whopay: A scalable and anonymous payment system for peer-to-peer environments. In *26th IEEE International Conference on Distributed Computing Systems (ICDCS'06)*, pp. 13–13. 2006 (2006). https://doi.org/10.1109/ICDCS.2006.85
34. Martinez-Pelaez, R., Rico-Novella, F., Satizabal, C.: Mobile payment protocol for micropayments: Withdrawal and payment anonymous. In *2008 New Technologies, Mobility and Security*, pp. 1–5. 2008 (2008). https://doi.org/10.1109/NTMS.2008.ECP.61
35. Miers, I., Garman, C., Green, M., Rubin, A.D.: Zerocoin: Anonymous distributed e-cash from bitcoin. In *2013 IEEE Symposium on Security and Privacy*, pp. 397–411. 2013 (2013). https://doi.org/10.1109/SP.2013.34
36. Ben Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy*, pp. 459–474. 2014 (2014). https://doi.org/10.1109/SP.2014.36
37. Miao, J., Han, Z.: An decentralized anonymous payment confidential transactions with efficient proofs and scalability. In *2022 IEEE International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA)*, pp. 1347–1351. 2022 (2022). https://doi.org/10.1109/EEBDA53927.2022.9744784
38. Kwansah Ansah, A.K., Adu-Gyamfi, D., Anokye, S.: Privacy preservation of users in p2p e-payment system. In *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pp. 1–8. 2019 (2019). https://doi.org/10.1109/ICECCT.2019.8869354
39. Isaac, J.T., Zeadally, S.: An anonymous secure payment protocol in a payment gateway centric model. Procedia Computer Science **10**, 758 (2012). https://doi.org/10.1016/j.procs.2012.06.097. ANT 2012 and MobiWIS 2012
40. Chen, S.W., Tso, R.: Nfc-based mobile payment protocol with user anonymity. In *2016 11th Asia Joint Conference on Information Security (AsiaJCIS)*, pp. 24–30. 2016 (2016). https://doi.org/10.1109/AsiaJCIS.2016.30
41. Pfitzmann, A., Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf (2010)
42. Edman, M., Yener, B.: On Anonymity in an Electronic Society: A Survey of Anonymous Communication Systems. ACM Comput. Surv. **42**(1) (2009). https://doi.org/10.1145/1592451.1592456
43. Ren, J., Wu, J.: Survey on anonymous communications in computer networks. Computer Communications **33**(4), 420 (2010). https://doi.org/10.1016/j.comcom.2009.11.009
44. Li, B., Erdin, E., Gunes, M.H., Bebis, G., Shipley, T.: An overview of anonymity technology usage. Computer Communications **36**(12), 1269 (2013). https://doi.org/10.1016/j.comcom.2013.04.009
45. Hou, H., Ning, J., Zhao, Y., Deng, R.H.: A traitor-resistant and dynamic anonymous communication service for cloud-based vanets. IEEE Transactions on Services Computing **15**(5), 2551 (2022). https://doi.org/10.1109/TSC.2021.3071156
46. Yang, X., Yi, X., Nepal, S., Khalil, I., Huang, X., Shen, J.: Efficient and anonymous authentication for healthcare service with cloud based wbans. IEEE Transactions on Services Computing **15**(5), 2728 (2022). https://doi.org/10.1109/TSC.2021.3059856
47. Xu, H., Hsu, C., Harn, L., Cui, J., Zhao, Z., Zhang, Z.: Three-factor anonymous authentication and key agreement based on fuzzy biological extraction for industrial internet of things. IEEE Transactions on Services Computing pp. 1–14 (2023). https://doi.org/10.1109/TSC.2023.3257569
48. Wang, H., He, D., Yu, J., Wang, Z.: Incentive and unconditionally anonymous identity-based public provable data possession. IEEE Transactions on Services Computing **12**(5), 824 (2019). https://doi.org/10.1109/TSC.2016.2633260
49. Gheisari, M., Najafabadi, H.E., Alzubi, J.A., Gao, J., Wang, G., Abbasi, A.A., Castiglione, A.: Obpp: An ontology-based framework for privacy-preserving in iot-based smart city. Future Generation Computer Systems **123**, 1 (2021). https://doi.org/10.1016/j.future.2021.01.028
50. McCauley, N.P., Chi, Y., Yan, R.: Anonymous payment transactions (2021)
51. Canard, S., Malville, E., Traore, J., Cosnefroy, B., Caron, S.: Anonymous and secure internet payment method and mobile devices (2009)
52. Canard, S., Malville, E., Traore, J., Cosnefroy, B., Caron, S.: Anonymous and secure internet payment method and mobile devices (2008)
53. Stock, H.: Digicash idea finds new life in more flexible ecash. American Banker **165**(67), 9 (2000)
54. Mearian, L.: Lawmakers have introduced a bill that would allow the us treasury to create a digital dollar. Computerworld (Online Only) p. 1 (2022)
55. Tor Project Anonymity Online (2022). `www.torproject.org`
56. Haraty, R.A., Zantout, B.: The TOR data communication system. Journal of Communications and Networks **16**(4), 415 (2014). https://doi.org/10.1109/JCN.2014.000071
57. I2P Anonymous Network (2022). `https://geti2p.net`
58. Hoang, N.P., Kintis, P., Antonakakis, M., Polychronakis, M.: An Empirical Study of the I2P Anonymity Network and Its Censorship Resistance. In *Proceedings of the Internet Measurement Conference 2018*, IMC '18, pp. 379–392. Association for Computing Machinery, New York, NY, USA, 2018 (2018). https://doi.org/10.1145/3278532.3278565
59. Leszczyna, R.: A Review of Traffic Analysis Attacks and Countermeasures in Mobile Agents' Networks. In *Moving technology ethics at the forefront of society, organisations and governments*, ed. by Pelegrín-Borondo, J., Oliva, M.A., Murata, K., Palma, A.M.L., pp. 439–452.

Universidad de La Rioja, 2021 (2021). https://dialnet.unirioja.es/servlet/articulo?codigo=8037082
60. Raymond, J.F.: Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems, pp. 10–29. Springer Berlin Heidelberg, Berlin, Heidelberg, 2001 (2001). https://doi.org/10.1007/3-540-44702-4_2
61. Venkatesh, V., Morris, M., Davis, G., Davis, F.: User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly **27**, 425 (2003). https://doi.org/10.2307/30036540
62. Leszczyna, R.: Aiming at methods' wider adoption: Applicability determinants and metrics. Computer Science Review **40**, 100387 (2021). https://doi.org/10.1016/j.cosrev.2021.100387
63. Wolves, F.: 8 ways to get paid for leaving your computer running. https://financialwolves.com/get-paid-for-leaving-your-computer-running/ (2023). Accessed 10 January 2024
64. Weiss, R.J.: 12 legit ways to get paid for searching the web. https://www.thewaystowealth.com/make-money/get-paid-to-play-games/ (2023). Accessed 10 January 2024
65. StartedBlogging: 10 file sharing websites that pay for downloads. https://startedblogging.com/file-sharing-websites-that-pay-for-downloads/ (2023). Accessed 10 January 2024
66. Weiss, R.J.: Get paid to play games: The best apps, websites and jobs. https://www.thewaystowealth.com/make-money/get-paid-to-play-games/ (2023). Accessed 10 January 2024
67. Cruz, J.J.D.: Photomath: Earn $300 a week by solving math problems online. https://phmillennia.com/photomath-14/ (2023). Accessed 10 January 2024
68. MathforMoney: How to earn money by solving math problems. https://www.mathformoney.app/earn-money-solving-math-problems.html (2023). Accessed 10 January 2024
69. Gupta, R., Kumar, B., Banga, G.: Role of affiliate marketing in today's era: A review. INDIAN JOURNAL OF ECONOMICS AND DEVELOPMENT **13**(2A), 687 (2017). https://doi.org/10.5958/2322-0430.2017.00153.6
70. Mahdian, M., Tomak, K.: Pay-per-action model for online advertising. International Journal of Electronic Commerce **13**(2), 113 (2008). https://doi.org/10.2753/JEC1086-4415130205
71. Pelánek, R., Jarušek, P.: Student Modeling Based on Problem Solving Times. International Journal of Artificial Intelligence in Education **25**(4), 493 (2015). https://doi.org/10.1007/s40593-015-0048-x
72. Leszczyna, R.: TAmail – Anonymous Sending of Messages with Possibility of Responding. Tech. rep. (2023). Submitted to Information Systems and e-Business Management
73. Leszczyna, R.: Practical cybersecurity assessment techniques - why are they adopted? A Review, Determinants and the Applicability Checklist. Tech. rep. (2023). Submitted to IEEE Access
74. Syverson, P., Tsudik, G., Reed, M., Landwehr, C.: Towards an analysis of onion routing security. In *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*, ed. by Federrath, H., Lecture Notes in Computer Science, pp. 96–114. Springer-Verlag New York, Inc., Berkeley, California, USA, 2000 (2000)
75. Dolev, S., Ostrobsky, R.: Xor-trees for efficient anonymous multicast and reception. ACM Transactions on Information Systems Secururity **3**(2), 63 (2000)
76. Dlodlo, N., Mofolo, M., Masoane, L., Mncwabe, S., Sibiya, G., Mboweni, L.: Research Trends in Existing Technologies that are Building Blocks to the Internet of Things. In *Innovations and Advances in Computing, Informatics, Systems Sciences, Networking and Engineering*, ed. by Sobh, T., Elleithy, K., pp. 539–548. Springer International Publishing, Cham, 2015 (2015)
77. Hyman, V.: Your real-time guide to real-time payments. https://www.mastercard.com/news/perspectives/2022/real-time-payments-what-is-rtp-and-why-do-we-need-instant-pay (2023). Accessed 10 January 2024
78. LLP., D.: Economic impact of real-time payments. Technical report, Mastercard (2019)
79. Webster, N.: Webster's Revised Unabridged Dictionary. G. & C. Merriam Company, 1913 (1913)
80. Babylon Software: Babylon NG (2020). dictionary.babylon-software.com
81. Verkijika, S.F.: An affective response model for understanding the acceptance of mobile payment systems. Electronic Commerce Research and Applications **39**, 100905 (2020). https://doi.org/10.1016/j.elerap.2019.100905
82. Leszczyna, R.: Review of cybersecurity assessment methods: Applicability perspective. Computers & Security **108**, 102376 (2021). https://doi.org/10.1016/J.COSE.2021.102376
83. Wallis, T., Leszczyna, R.: Ee-isac – practical cybersecurity solution for the energy sector. Energies **15**(6) (2022). https://doi.org/10.3390/en15062170
84. Leszczyna, R., Wallis, T., Wróbel, M.R.: Developing novel solutions to realise the european energy – information sharing & analysis centre. Decision Support Systems **122**, 113067 (2019). https://doi.org/10.1016/j.dss.2019.05.007
85. Information Sharing & Analysis Centre (EE-ISAC). ww.ee-isac.eu