UDC 004.056.53
DOI https://doi.org/10.32782/EIS/2026-109-2

ATTRIBUTES AND METRICS OF TRUST BASED MODELS IN CLOUD SECURITY

Bobrenok Viacheslav Vitaliiovych,
Postgraduate Student at the Department of Information Technologies and Systems
National Metallurgical Academy of Ukraine
Ukrainian State University of Science and Technologies
ORCID ID: 0009-0009-4028-2173

Guda Anton Ihorovych,
Doctor of Technical Sciences,
Professor at the Department of Information Technologies and Systems
National Metallurgical Academy of Ukraine
Ukrainian State University of Science and Technologies
ORCID ID: 0000-0003-1139-1580

Cloud environments became a popular solution for hosting and managing infrastructure and data for businesses in different domains: cloud computing service providers' revenue in 2018 amounted to approximately 217 billion US dollars, in 2022 – 481 billion, and the forecast for 2028 includes a profit figure of more than 1 trillion US dollars. But as organizations migrate from traditional on-premises infrastructures to cloud platforms, conventional perimeter-based security approaches have become insufficient due to the absence of clear network boundaries and the rise of remote access. It introduced a new set of security challenges. For example, in 2021, losses to companies from the leakage of confidential information amounted to an average of 3.5 million US dollars, and losses from attacks aimed at destroying or damaging IT infrastructure amounted to 4.6 million US dollars. Thus, these issues must be resolved to facilitate further adoption of cloud technologies. Trust based models might be a solution for some of these challenges as the evolution of trust models in cloud security reflects a shift from static to dynamic and adaptive mechanisms. By shifting from implicit trust to continuous verification and contextual awareness, these models provide a more robust framework for protecting sensitive information and maintaining secure access in cloud ecosystems.

This work is an attempt to discover key attributes of trust based models and how they can be used to create a mechanism for securing data and workloads in cloud environments. It is achieved by conducting an extensive review of existing security threats in cloud environments as well as a systematic analysis of key characteristics of trust based models and their applicability for mitigation of these threats.

*As a result, this work discovers key attributes of trust based models which can be used to implement new security mechanisms for cloud environments. Such mechanisms should be better suited for handling the dynamic nature of such environments. Even though **s**ecuring cloud environments remains a complex task, the attributes described in this research can be used to create new tools and methodologies which can greatly simplify it and facilitate further adoption of cloud technologies.*

Key words: *cloud computing, cyber security, cloud environments, trust based model.*

Бобренок Вячеслав, Гуда Антон. Атрибути та метрики моделей на основі довіри для захисту хмарних середовищ

Хмарні середовища стали популярним рішенням для розміщення та управління інфраструктурою й даними для бізнесу в різних сферах: дохід постачальників послуг хмарних обчислень у 2018 р. склав приблизно 217 мільярдів доларів США, у 2022 р. – 481 мільярд, а прогноз на 2028 р. включає показник прибутку понад 1 трильйон доларів США. Але по мірі того, як організації мігрують від традиційних локальних інфраструктур до хмарних платформ, традиційні підходи до безпеки на основі периметра стали недостатніми через відсутність чітких меж мережі та зростання популярності віддаленого доступу. Це призвело до появи нового набору проблем безпеки. Наприклад, у 2021 р. збитки компаній від витоку конфіденційної інформації становили в середньому 3,5 мільйона доларів США, а збитки від атак, спрямованих на знищення або пошкодження IT-інфраструктури, становили 4,6 мільйона доларів США. Таким чином, ці проблеми необхідно вирішити, щоб сприяти подальшому розвитку хмарних технологій. Моделі, засновані на довірі, можуть бути рішенням деяких із цих проблем, оскільки еволюція моделей довіри в хмарній безпеці відображає перехід від статичних до динамічних та адаптивних механізмів. Переходячи від неявної довіри до постійної перевірки та контекстної обізнаності, ці моделі забезпечують більш надійну основу для захисту конфіденційної інформації та підтримки безпечного доступу в хмарних екосистемах.

Ця робота є спробою виявити ключові атрибути моделей, заснованих на довірі, та те, як їх можна використовувати для створення механізму захисту даних та робочих навантажень у хмарних середови-

щах. Це досягається шляхом проведення ретельного огляду існуючих загроз безпеці в хмарних середовищах, а також систематичного аналізу ключових характеристик моделей, заснованих на довірі, та їхньої застосовності для зменшення цих загроз.

У результаті, ця робота виявляє ключові атрибути моделей, заснованих на довірі, які можна використовувати для впровадження нових механізмів безпеки для хмарних середовищ. Такі механізми повинні краще підходити для обробки динамічної природи таких середовищ. Незважаючи на те, що захист хмарних середовищ залишається складним завданням, атрибути, описані в цьому дослідженні, можна використовувати для створення нових інструментів та методологій, які можуть значно спростити його та сприяти подальшому впровадженню хмарних технологій.

Ключові слова: *хмарні обчислення, кібербезпека, хмарні середовища.*

Relevance of the problem. Cloud environments offer access to scalable computing resources on demand over the Internet. The opportunities that this provides are too attractive for consumers to ignore. For example, cloud computing service providers' revenue in 2018 amounted to approximately 217 billion US dollars, in 2022 – 481 billion, and the forecast for 2028 includes a profit figure of more than 1 trillion US dollars. However, such a rapid growth in the popularity of cloud environments requires special attention to the security of resources and data located in the cloud. After all, the cloud computing paradigm also has disadvantages, in particular its opaque nature, which leads to significant trust and security issues that hinder its development and spread. All these vulnerabilities create new challenges in the field of cybersecurity and can lead to significant financial and reputational losses. Thus, in 2021, losses to companies from the leakage of confidential information amounted to an average of 3.5 million US dollars, and losses from attacks aimed at destroying or damaging IT infrastructure amounted to 4.6 million US dollars [1].

There are a few models which can be used to secure data and infrastructure in cloud environments. One of them is Perimeter-Based Security which relies on the concept of a trusted internal network protected by a secure boundary (e.g., firewalls, VPNs). Once users gain access to the internal network, they are typically granted broad permissions. While this model is simple and cost-effective, it is increasingly inadequate in cloud environments where users access resources from multiple locations, applications are distributed across platforms and insider threats are more prevalent. Another solution might be Role-Based Access Control (RBAC) which assigns access rights based on predefined organizational roles. Users are granted permissions according to their role. But while being simple and easy to implement, such a mechanism lacks contextual awareness and has limited flexibility in dynamic environments. Also it might lead to such an amount of different roles for large organizations, that can be difficult to manage. Attribute-Based Access Control (ABAC) extends access control by incorporating multiple attributes, including user characteristics, resource types, and environmental conditions. That adds support for context sensitivity (time, device, location, etc) and increases flexibility, but introduces even more complexity in policy design and management, making it more challenging to implement and audit. There are also Cryptographic Security Models which focus on securing data through mathematical techniques such as encryption and digital signatures. However, they do not address access control directly and must be integrated with other models for comprehensive security.

In this work we will focus on another type of models – Trust-Based Models. Trust-based models in cloud security define how much confidence a system places in users, devices, and services when granting access to resources. Such models incorporate contextual information – such as user behavior, device status, and geographic location – to dynamically adjust security requirements in real time. They operate on the principle that trust is not implicit but continuously evaluated. As a result, these models are particularly effective in cloud environments due to their ability to handle remote access, multi-cloud deployments, and insider threats. However, their implementation is complex and requires advanced infrastructure, including identity providers, policy engines, and monitoring systems.

Related works. Trust management technologies have been widely investigated in many fields including economics, sociology, and computer science [2; 3, p. 552–573; 4, p. 403–420]. The main focus of such works in computer science is usually aimed at solving security and privacy related issues. For example, the TNA-SL algorithm [5, p. 179–184] is a well-known trust management algorithm in P2P networks. This algorithm represents the trust network between peers as a cycle-free directed sequential parallel graph (DSPG), which prevents the creation of multiple paths between each pair of peers. The simplification of graphs and the definition of trust are based on subjective logic, according to which the opinions of each participant in the system about others are measured and stored.

The strength of this algorithm lies in the accuracy of trust information and the clear definition of negative trust. Known disadvantages of this algorithm include its long execution time due to the frequent matrix multiplication required to determine the location of a trusted peer, the loss of some trust information to avoid cycles in the graph, and limited network scalability. Rao S. et al. [6, p. 822–825] introduced an extended subjective logic for trust management (ESL-TM) in P2P networks. This involves a new trust factor – the decay factor – which is used as part of the punishment mechanism after a transaction with a negative rating. Kurdi H. et al. [7, p. 3534–3554] presented the InterTrust algorithm as a potential tool for trust management in federated cloud environments, which improves the TNA-SL algorithm, in particular in terms of scalability and execution time. This modification makes the TNA-SL algorithm more suitable for the case of federated cloud environments. The InterTrust algorithm eliminates the complexity, in terms of execution and space, associated with the two n×n matrices required for the TNA-SL algorithm. In addition, InterTrust cumulatively stores all previous trust information between peers to overcome the loss of trust information in the original algorithm. Another algorithm based on extended subjective logic is proposed by Hu Z. et al. [8, p. 380–384]. The Organization Domain Trust Model for Federations (ODTMF) aims to estimate the trust values of organization domains using a new operator called the weight operator to show the different influence of each member of an organization federation.

A trust management framework was developed by Khan S. M. et al. [9, p. 494–501] and Shvachko K. et al. [10, p. 1–10] specifically for Hadoop clouds. To achieve high scalability, all trust calculations are formulated and executed as distributed cloud computing. Parameters such as initiation time, cost, processing speed, error rate, and bandwidth are used to calculate trust values, which are periodically updated to ensure that trusted resources can be assigned to users with higher trust values.

Abrams Z. [11, p. 21–30], presented a domain-based trust model in the framework of cloud security. The focus is on filtering unreliable trust feedback to make systems more reliable. A fuzzy logic technique called Fuzzy ART is proposed by Jaiganesh M. et al. [12, p. 341–348] that exploits the trust of virtual machines in cloud environments.

The purpose of this work is to discover key attributes of trust based models and how they can be used to create a robust mechanism for securing data and workloads in cloud environments.

Trust. Trust is a measure used to assess social actors in terms of mutual benefits, coordination, and cooperation. Individuals continually adjust their level of trust in others as their perceptions change through direct interactions and through the beliefs and opinions shared by those around them. Trust is a crucial fact that affects decisions of an object to interact with another object. We can find examples of such decisions in our everyday life. When purchasing a specific product, we may favor certain brands due to our trust that these brands will provide better quality than others. This trust may come from our previous experience in using these brands' products or from feedback or recommendations of other people.

In analogy to the above example, trust also affects decisions of components in a cloud environment to interact with each other. However, machine objects are not able to perceive other objects around them the same way humans do, so building trust in cloud environments is much more difficult. Furthermore, it is difficult to measure the exact trust value of an object because each object might have a different interpretation and perception of the term "trustworthy". One object can acknowledge some service as "very trustworthy" for a specific interaction that it has had, but another object might see the same service as "untrustworthy" for a similar interaction.

Therefore, it is essential to have a clear definition of trust, we suggest using the following definitions in the context of a information technologies in this paper [13]:

- *Trust* is a qualitative or quantitative property of a trustee, evaluated by a trustor as a measurable belief, in a subjective or objective manner, for a given task, in a specific context, for a specific time period.
- *Trust model* includes three trust metrics (TM): Knowledge, Experience, and Reputation. Each TM consists of several trust attributes (TAs). Each TA represents the trustworthiness feature of a trustee.

In the definitions above, the **trustor** refers to the entity that is expected to initiate an interaction with another entity, while the **trustee** denotes the entity that provides the necessary information to the trustor. Since trust can be measured in either quantitative or qualitative terms, its assessment may involve not only well-known numerical metrics such as similarity and accuracy, but also other forms of evaluation such as similarity, accuracy, etc., we can use qualitative properties like motivation, awareness, and commitment to judge certain situations in the process of trust based decision making. It is also important to recognize trust as a belief even in the cyber world. That means, trust

is relative and 100 percent accuracy is neither practical nor achievable in diverse environments like cloud ones. Moreover, the perception of trust can be either subjective or objective, depending on requirements and available information. The last thing to emphasize is that trust is a relative quantity between two or more objects in contrast to a measurement of individual objects.

Trust metrics. As mentioned above, the trust model includes three trust metrics: Knowledge, Experience, and Reputation. So now we should provide descriptions of these metrics to describe the model further.

The knowledge TM provides a perception about a trustee before an interaction. To make trust based decisions possible, we must have relevant data for its assessment. This data can include social relationships like co-work, credibility factors like cooperativeness, time dependent features like frequency and duration of interactions, and spatial distribution of relevant trustees compared to the trustor.

Reputation TM can be seen as a rewarding system which tracks the history of interactions originated by the trustee. It can be used to either encourage or discourage further interactions with a particular trustee based on the history of its prior interactions.

After gathering enough data about trustees through the knowledge TM, it can be used by the trustor to initiate interactions with trustees which seems to be trustworthy. However, the results of these interactions might eventually change, so the experience TM can be used to keep track of each new interaction, accumulating experience for different contexts, tasks and times. It can be used to build up additional intelligence compared to the knowledge TM, so the future decision making can be improved. Such experience might include a feedback for each interaction or just a boolean value indicating whether an interaction was successful or not. This experience can then be shared between different objects to update the reputation TM.

In summary, the experience TM considers only interactions between a trustor and a trustee, whereas the reputation TM is about the global appearance of the trustee. Meanwhile knowledge TM is used as the building block for both of those metrics.

Trust attributes. Even though cloud environments produce a large amount of data, not all of it can be used for the trust evaluation. As a result, interaction logs can be used to extract different trust attributes and store them in a data repository for further analysis. Hence, we need to create a numerical model that can extract these basic features. To achieve it, lets define the assessment of knowledge (*K*) towards an object *j* by an object *i* at time *t* as $K_{ij}^{x}(t)$, where x represents one of the features:

- Co-work relationship (CWR).
- Mutuality and Centrality (MC).
- Cooperativeness-Frequency-Duration (CFD).
- Reward.

Co-work relationship (CWR) can be used to characterize objects that are collaborating in a common cloud environment. In such a situation, we focus on working relationships in a particular service domain. To measure it, we compare interactions between a trustor and a trustee, as calculated in the Formula 1:

$$K_{ij}^{CWR}(t)=\frac{\left|c_{ij}^{I}\right|}{\left|c_{j}^{I}\right|}, \quad (1)$$

where c_{ij}^{I} is the vector of interactions between trustor i and trustee j, and c_{j}^{I} is the vector of interactions originated at *j*. The symbol |.| represents the determinant of a vector. K_{ij}^{CWR} represents a relative measurement of shared interactions to total interactions originated at the trustee.

It is reasonable to expect more collaboration between objects if they have a history of frequent and long interactions. As a result, we can get values for cooperativeness, frequency, and duration (CFD) trust attribute using Formula 2:

$$K_{ij}^{CFD}=\sum_{m=1}^{n}\frac{c_m}{t_m}E(c_m). \quad (2)$$

Here, c_1, c_2, …, c_n is a set of interactions over some period in which the trustor is interested. c_m is the length of mth successful interaction between the trustor and the trustee and t_m is the total length of m interactions of the trustee. $E(c_m)$ is the binary entropy function which measures the balance in the interaction and can be calculated with Formula 3:

$$E(c_m)=-p\log p-(1-p)\log(1-p), \quad (3)$$

where *p* is the fraction of the interactions between the trustor and the trustee. $E(c_m)$ follows a binary distribution as stated in (D. J. MacKay, 2003). It is evident that the maximum entropy (i.e., $E(c_m)=1$) is reachable only when $p=0:5$ that is 50 percent contribution from each party.

Then it is important to have a feedback model in order to assess the historical experiences of interactions between a trustor and a trustee, as it is critical to maintain the maximum trustworthiness levels. To achieve it we use the following exponential downgrading Formula 4.

$$K_{ij}^{RS}(t)=\frac{\|C\|-\|C_p\|}{\|C\|}e^{\frac{\|C_p\|}{\|C\|}}. \quad (4)$$

Here, ||*C*|| is the total number of interactions during a period *t*, and ||C_p|| the total number of unsuccessful or suspicious interactions. To penalize misbehavior, the slope of the distribution is increased in comparison to the standard exponential distribution. As a result, a greater number of malicious interactions leads to a lower reward value.

It is intuitive to assume that a greater number of shared objects indicates a higher level of similarity between them. However, mutuality alone cannot be used as a TA, since the number of mutual friends is proportional to the total number of friends each object has. As a result, an object with many friends gains an additional advantage over an object that has recently joined the network, even if the latter is more trustworthy. To avoid such situations, a relative measure of mutuality with respect to the total number of friends is used instead. This is essentially the centrality property of the trustee and is calculated using Formula 5:

$$K_{ij}^{MC}(t)=\frac{|M_{ij}|}{|N_i|}, \quad (5)$$

where M_{ij} is the set of common friends between *i* and *j*, and N_i is the set of trustee's friends.

Conclusions. Securing cloud environments remains a complex task, but the set of trust attributes described in this paper can be used to implement new security mechanisms for cloud environments. Such mechanisms should be better suited for handling the dynamic nature of such environments. Our next steps will be to use available technologies to gather and store data required to calculate values of these attributes. Once this data is ready we can use it to implement an algorithm for making trust based decisions for interactions between components of cloud environments. Then the focus will be on improving accuracy of this algorithm and optimizing it so it can be used in real world use cases.

BIBLIOGRAPHY:

1. Cost of a Data Breach Report 2021. IBM. URL: https://info.techdata.com/rs/946-OMQ-360/images/Cost_of_a_Data_Breach_Report_2021.PDF (дата звернення: 20.09.2024).

2. Marsh S. P. Formalising trust as a computational concept: PhD dissertation. Stirling: University of Stirling, 1994.

3. Huang F. Building social trust: A human-capital approach. Journal of Institutional and Theoretical Economics. 2007. Vol. 163, No. 4. P. 552–573. DOI: https://doi.org/10.1628/093245607783242981

4. Møllering G. The nature of trust: From Georg Simmel to a theory of expectation, interpretation and suspension. Sociology. 2001. Vol. 35, No. 2. P. 403–420. DOI: https://doi.org/10.1177/S0038038501000190

5. Jøsang A., Bhuiyan T. Optimal trust network analysis with subjective logic. Proceedings of the 2nd International Conference on Emerging Security Information Systems and Technologies. IEEE, 2008. P. 179–184. DOI: https://doi.org/10.1109/SECURWARE.2008.64

6. Rao S., Wang Y., Tao X. L. The comprehensive trust model in P2P based on improved EigenTrust algorithm. Proceedings of the International Conference on Measuring Technology and Mechatronics Automation. IEEE, 2010. P. 822–825. DOI: https://doi.org/10.1109/ICMTMA.2010.221

7. Kurdi H. et al. A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments. The Journal of Supercomputing. 2019. Vol. 75. P. 3534–3554. DOI: https://doi.org/10.1007/s11227-018-2669-y

8. Hu Z., Liu L., Wang C. Organization domain trust evaluation model in a federated environment based on subjective logic. Proceedings of the International Conference on Information Technology, Computer Engineering and Management Sciences. IEEE, 2011. P. 380–384. DOI: https://doi.org/10.1109/ICM.2011.62

9. Khan S. M., Hamlen K. W. HATMAN: Intra-cloud trust management for Hadoop. Proceedings of the 5th International Conference on Cloud Computing. IEEE, 2012. P. 494–501. DOI: https://doi.org/10.1109/CLOUD.2012.64

10. Shvachko K. et al. The Hadoop distributed file system. Proceedings of the 26th Symposium on Mass Storage Systems and Technologies. IEEE, 2010. P. 1–10. DOI: https://doi.org/10.1109/MSST.2010.5496972

11. Abrams Z., McGrew R., Plotkin S. A non-manipulable trust system based on EigenTrust. ACM SIGecom Exchanges. 2005. Vol. 5, No. 3. P. 21–30. DOI: https://doi.org/10.1145/1120717.1120721

12. Jaiganesh M., Aarthi M., Kumar A. V. A. Fuzzy ART-based user behavior trust in cloud computing. Artificial Intelligence and Evolutionary Algorithms in Engineering Systems. New Delhi: Springer, 2015. P. 341–348.

13. International Telecommunication Union. Overview of trust provisioning for information and communication technology infrastructures and services (ITU-T Recommendation Y.3052). 2017.

REFERENCES:

1. *Cost of a Data Breach Report 2021*. IBM. URL: https://info.techdata.com/rs/946-OMQ-360/images/Cost_of_a_Data_Breach_Report_2021.PDF

2. Marsh, S. P. (1994). Formalising trust as a computational concept. PhD dissertation. Dept. of Computer Science and Mathematics, University of Stirling, Scotland, UK.

3. Huang, F. (2007). Building social trust: A human-capital approach. *Journal of Institutional and Theoretical Economics*, 163(4), 552–573. DOI: https://doi.org/10.1628/093245607783242981

4. Møllering, G. (2001). The nature of trust: From Georg Simmel to a theory of expectation, interpretation and suspension. *Sociology*, 35(2), 403–420. DOI: https://doi.org/10.1177/S0038038501000190

5. Jøsang, A., & Bhuiyan, T. (2008). Optimal trust network analysis with subjective logic. In *Proceedings of the 2nd International Conference on Emerging Security Information Systems and Technologies* (pp. 179–184). IEEE, Cap Esterel, France. DOI: https://doi.org/10.1109/SECURWARE.2008.64

6. Rao, S., Wang, Y., & Tao, X. L. (2010). The comprehensive trust model in P2P based on improved EigenTrust algorithm. In *International Conference on Measuring Technology and Mechatronics Automation* (pp. 822–825). IEEE, Changsha, China. DOI: https://doi.org/10.1109/ICMTMA.2010.221

7. Kurdi, H., Alfaries, A., Al-Anazi, A., et al. (2019). A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments. *The Journal of Supercomputing*, 75, 3534–3554. DOI: https://doi.org/10.1007/s11227-018-2669-y

8. Hu, Z., Liu, L., & Wang, C. (2011). Organization domain trust evaluation model in a federated environment based on subjective logic. In *Proceedings of the International Conference on Information Technology, Computer Engineering and Management Sciences* (pp. 380–384). IEEE, Nanjing, China. DOI: https://doi.org/10.1109/ICM.2011.62

9. Khan, S. M., & Hamlen, K. W. (2012). HATMAN: Intra-cloud trust management for Hadoop. In *Proceedings of the 5th International Conference on Cloud Computing* (pp. 494–501). IEEE, Honolulu, USA. DOI: https://doi.org/10.1109/CLOUD.2012.64

10. Shvachko, K., Kuang, H., Radia, S., & Chansler, R. (2010). The Hadoop distributed file system. In *Proceedings of the 26th Symposium on Mass Storage Systems and Technologies* (pp. 1–10). IEEE, Incline Village, USA. DOI: https://doi.org/10.1109/MSST.2010.5496972

11. Abrams, Z., McGrew, R., & Plotkin, S. (2005). A non-manipulable trust system based on EigenTrust. *ACM SIGecom Exchanges*, 5(3), 21–30. DOI: https://doi.org/10.1145/1120717.1120721

12. Jaiganesh, M., Aarthi, M., & Kumar, A. V. A. (2015). Fuzzy ART-based user behavior trust in cloud computing. In *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems* (pp. 341–348). Springer, New Delhi.

13. International Telecommunication Union (2017). *Overview of trust provisioning for information and communication technology infrastructures and services* (ITU-T Recommendation Y.3052).

Дата першого надходження статті до видання: 06.03.2026
Дата прийняття статті до друку після рецензування: 02.04.2026
Дата публікації (оприлюднення) статті: 29.05.2026