Establishing a Zero Trust Strategy in Cloud Computing Environment

Conference Paper · January 2020

DOI: 10.1109/ICCCI48352.2020.9104214

2 authors:

Saima Mehraj
University of Kashmir
5 PUBLICATIONS **73** CITATIONS
SEE PROFILE

M. Tariq Banday
University of Kashmir
156 PUBLICATIONS **708** CITATIONS
SEE PROFILE

Establishing a Zero Trust Strategy in Cloud Computing Environment

Saima Mehraj
Department of Electronics and Inst. Technology
University of Kashmir, Srinagar, India
saimamehraj@kashmiruniversity.net

M. Tariq Banday
Department of Electronics and Inst. Technology
University of Kashmir, Srinagar, India
sgrmtb@yahoo.com

***Abstract*— The increased use of cloud services and its various security and privacy challenges such as identity theft, data breach, data integrity and data confidentiality has made trust management, which is one of the most multifaceted aspect in cloud computing, inevitable. The growing reputation of cloud computing technology makes it immensely important to be acquainted with the meaning of trust in the cloud, as well as identify how the customer and the cloud service providers establish that trust. The traditional trust management mechanisms represent a static trust relationship which falls deficit while meeting up the dynamic requirement of cloud services. In this paper, a conceptual zero trust strategy for the cloud environment has been proposed. The model offers a conceptual typology of perceptions and philosophies for establishing trust in cloud services. Further, importance of trust establishment and challenges of trust in cloud computing have also been explored and discussed.**

Keywords— Zero Trust Strategy; Trust Management System; Incipient Technology; Objective Trust; Subjective Trust.

I. INTRODUCTION

Cloud computing is an incipient technology that has endured a rapid development in recent years. Since last decade, the technology has witnessed persuasive upsurge not just for the reason it offers various services and amenities to organizations, but it relieves organizations from the burden of installations, licensing, training, and maintenance hitches [1]. Moreover, cloud computing delivers its services from remote data centers over the network, and therefore, data owner has no control over the data and its location, so it becomes essential for the cloud consumer to have trust on cloud and its provider.

Indeed, trust is a complicated social phenomenon that involves risk and dependence of one party on another to develop confidence-based relationships in a diverse environment. Although, trust has been studied in various fields, yet there is no widely accepted definition among academicians and researchers. In general, trust is defined using the terms—expectancy, belief, and willingness to take risk [2]. Moreover, trust substantiates to be an essential facilitator for building successful relationships and therefore, provides an efficient technique for improving the security. Besides, it is often believed that it can impact security by helping in decision-making processes. Trust is a complex and broad notion which includes objective and subjective trust properties. The subjective trust properties include willingness, previous history, and honesty. In addition, the objective properties influencing the trust include reliability, behavior, and reputation [3].

Establishing trust in cloud computing is an essential aspect that is yet to receive satisfactory consideration from industry as well as academia. Notably, trust is a most critical feature of cloud computing. Furthermore, establishing trust in cloud signifies that one has faith and is willing to depend on the cloud service and its provider. Trust, therefore, is a considerable indicator for selecting the authenticated user and recommending a trusted service in cloud computing [4]. Hence, trust in cloud computing is believed to be a degree of reputation and measure of trust between a cloud user and a cloud service provider (CSP).

Besides, a comprehensively discussing trust, its management and issues in cloud computing scenario, the main contribution of this paper is the proposal of a conceptual model namely zero trust model for trust-based authorization system in cloud computing paradigm.

Following this introduction, section II presents a literature review related to the current study; section III defines the trust management in cloud computing; section IV elaborates the proposed model; and section V discusses the findings of the research which is followed by conclusion and further work.

II. LITERATURE REVIEW

Since trust in cloud computing, an active area of research, cannot be acquired easily, yet is an artifact of relationship and can be earned over time. Various researchers are at work in finding a robust and efficient trust strategy in cloud computing paradigm. Many trust architectures, models and frameworks have been proposed to develop confidence-based relationships between cloud customer and CSP. Some of the remarkable works in this field are discussed in this section.

Abbadi and Martin in [5], presented a cloud taxonomy to well understand the requirements for providing trustworthy middleware services which the authors believe helps in establishing trust in cloud. It provides many stages of transparency in the context of technical complexities and establishing trust. Additionally, the authors have also explored the cloud operational trust properties which includes, Adaptability, Resilience, Scalability, Reliability and Availability. In this work, the authors have summarized the properties of cloud infrastructures which could be used to evaluate the trustworthiness of cloud operation. Matin and Jafari in [6], analyzed various number of trust evaluation mechanisms used in the cloud environment so far. The authors have compared the trust evaluation frameworks on the basis of various factors which includes; integrity, security, dependability, scalability, dynamicity and so forth. Furthermore,

978-1-7281-4514-3/20/$31.00 ©2020 IEEE

the authors present a systematic and comprehensive research on the state-of-the-art trust evaluation mechanisms which is quite rare in cloud environment and will support professionals, academics, and researchers in their understanding of trust evaluation schemes in the cloud paradigm. Shaikh and Sasikumar in [7], presented a trust model that measures the security strength of cloud services and computes a trust value. The defined trust model can be efficiently embraced by the cloud users to select a particular cloud service. As per the authors, the proposed trust model can be used by the cloud providers as a benchmark to find out the shortcomings as well as improvements of a cloud service. Albert and Rajeev in [8], investigated the trust related issues of the cloud user in CSP with the security of their applications, data and resources. Moreover, the authors in this work are making an effort to outline the trust issue and suggest how CSP's may overcome trust issues. The assumption made in this work is that cloud users trust cloud computing only to the extent that the risk is observed to be low. Archana and Meenu in [9], presented a novel trust model for infrastructure service of cloud computing which is based on the security checks through standards and certifications. In addition, the authors have listed the factors that are significant for IAAS security. The presented trust framework calculates the trustworthiness of the cloud provider on the basis of security analysis through standards and certification accomplished by the cloud provider. P. Prakash et al. in [10], discussed the classification of various layers of cloud environment in this work. The authors also inspect the measurement of trust value for CSPs using fuzzy logic centroid method of defuzzification thus, suggesting a more proficient trust model. Moreover, the authors have used three parameters which includes, availability, turnaround time and reliability for evaluating trust. Therefore, the strength and security of cloud service is enhanced using this trust model. As a result, this model is more convenient and the trust is evaluated using a smaller number of parameters. Ritu et al. in [11], highlighted the significance of trust in cloud environment. The authors identified that trust is a vital factor in cloud computing as it provides security to the cloud environment. In addition, trust helps a user choose a reliable service and a CSP decide on a trusted user. Furthermore, the authors conduct a systematic literature survey of trust management. Also, the existing trust models are presented in order to evaluate trust based on number of parameters. In this work a brief description of fuzzy logic-based trust model in cloud has been discussed.

III. TRUST MANAGEMENT IN CLOUD COMPUTING

In this section, the significance of establishing trust in cloud computing is elucidated. In cloud paradigm, the CSP and the customer perhaps initiate communications with each other without having any previous interactions. As a result, lack of previous understanding and experience between a particular CSP and customer often leads to the insufficient information for consistently envisaging the trustworthiness of the customers and its CSP. Thus, lack of insufficient information and no prior transactions may result in mistrust [12, 13]. Moreover, trust turns out to be an indispensable mechanism in the facilitation of decision-making in cloud computing. Besides, trust challenges and issues become very critical when data storage and processing is decentralized across geographically dispersed data centers and similarly resources are distributed as well. Therefore, an efficient trust management is enforced to allow CSPs and customers fully trust each other and embrace the benefits of cloud computing.

The trust models [14, 15, 16, 17] are quite convenient for making efficient decisions in service-oriented environments such as cloud computing for selection of trustworthy entities. In essence, these trust models mostly take into consideration the past and present interaction experiences, behavioral observations, and recommendation when selecting trustworthy service providers and reliable customers. As a matter of fact, cloud computing offers massively distributed and greatly complex system which is non-transparent and therefore, highly abstracted. In consequence of this distributed and service-oriented architecture of cloud computing, the cloud customers need to reconsider parameters which are beyond the usual quality of service parameters for selecting the trustworthy entities.

Trust models are heterogeneous as they are distinct for different environments, frameworks, applications and contexts. Establishing the dynamic trust model for cloud services is a multidimensional task as the provisioning and de-provisioning of services in cloud are done dynamically. Moreover, trust management schemes are intended mainly for a specific application. Thus, traditional trust management mechanisms are most unsuitable for cloud paradigm because of cloud's service-oriented architecture [3].

A. Trust Management Challenges for Cloud Environment

The trust management mechanism for cloud environment introduces some of the challenges which are discussed as follows for consideration [12]:

i) Customization of trust in cloud paradigm brings in a great challenge as it let users to define the parameters from their point of view to establish trust. Moreover, the users weight the parameters as per their preferences. Therefore, the challenge turns out to be that up to what level the customization should be supported. Additionally, trust possesses two relationships: objective trust and subjective trust. The objective trust gives a global trust value whereas the subjective trust is local and changes with entities.

ii) Aggregation of trust information brings another challenge wherein the trust related information can be stored using two fundamental methodologies. The first approach to host the trust information is centralized approach; and the other one is decentralized approach. Both the methods have distinct number of pros and cons. In addition to this, aggregation of objective parameters (e.g., expert ratings or real-time measurements) and subjective parameters (e.g., recommendations by other users) is a big challenge.

iii) Trust evaluation includes various number of approaches such as, Black-box approach, Inside-out, and Outside-in approach. All the mentioned approaches have separate technique for trust evaluation. Hence, the efficient approach is required to be leveraged in cloud paradigm.

iv) Trust assessment is fairly essential for making any authorization decisions in trust-based access control of cloud

computing. However, the critical challenge in trust assessment is the reasonable and unbiased assignment of weights to different recommending trust factors or the parameters that are involved in trust assessment. Therefore, dynamic adaptability in weight assignment of trust assessment is prerequisite in cloud computing.

v) During trust establishment process, one has to contemplate the qualitative and quantitative information can be derived from distinct roots when incorporating multiple parameters into a trust model. The combination of information from different roots is a major challenge in cloud computing.

IV. ZERO-TRUST MODEL: THE MODERN APPROACH TO CYBER SECURITY

The Zero-Trust approach is a strategic initiative, rooted in the principle of "never trust, always verify". It refers to a security threat model with no assumption that the users, devices, data, applications and services that operate from within the security limit of an organization should be automatically trusted, instead before granting access, the system must verify each and every entity that requests for a connection to its resources, each and every time the user attempts to interact with the system thereby, asserting all the network traffic to be considered as untrusted. More importantly, Zero-Trust model benefits to prevent effective data breaches caused due to exploitation of privileged credentials by stamping out the concept of trust from an organization's network architecture. Furthermore, it is intended to safeguard modern digital environments by leveraging network micro-segmentation, simplifying granular user-access control, and preventing lateral movements. However, Zero-Trust model is all about eliminating trust from a system rather than deeming a system as trusted [18].

In essence, Zero-Trust is a security framework that contributes to secure on premise or cloud resources by eradicating unknown users and unmanaged devices and limiting all kinds of lateral movement. Zero Trust relies on technologies that include IAM (Identity and Access Management), data encryption, device verification, and multi-factor authentication (MFA). Moreover, implementing this model requires that all components inside and outside the network must be validated and proven trustworthy. In addition, principle of least privilege is enforced when access is granted by means of this security framework and restriction is imposed to the user access to only those resources that are authorized for each and every user, thus minimizing the risk of lateral movement across the environment [19].

V. THE PROPOSED MODEL

In this section, we propose Zero-Trust security model for cloud computing environment in order to address the modern security challenges that come up with cloud infrastructure. As a matter of fact, cloud-based services have changed the technology landscape for the modern enterprises. Also, security is the major challenge in deploying new infrastructure into the cloud. However, traditional security strategies (perimeter-centric) failed to make available the satisfactory control, visibility, and protection of user and application traffic. Therefore, Zero-Trust is proposed as the best fit for cloud deployments for the reason that cloud environment cannot be trusted so easily due to its dynamic and sharable landscape. To advance cloud security, the Zero-Trust strategy creates a record of what it has in the cloud and accordingly implements strong access control.

Zero-Trust being strategic initiative facilitates security leaders and decision makers to accomplish logical security implementations. Moreover, Zero-Trust has the capability to basically change the efficiency of security and data sharing across cloud infrastructure. From a security viewpoint, Zero-Trust framework can better track and block external attackers, while limiting security breaches resulting from insider attacks in cloud paradigm. From a data sharing viewpoint, Zero-Trust can better accomplish access privileges for users and devices across cloud environment to enable secure sharing. In addition, Zero-Trust scheme in cloud computing requires to integrate and incorporate a challenging combination of practices, policies, and technologies to succeed. However, figure 1 provides a basic principle of Zero-Trust strategy.

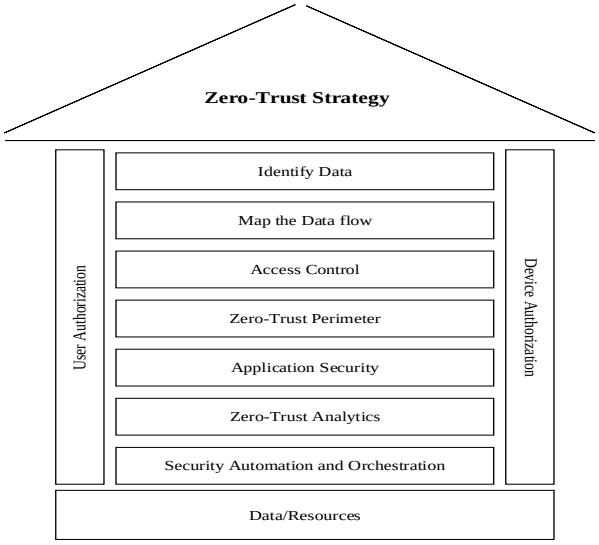

FIG. 1. THE BASIC CONCEPT OF ZERO-TRUST STRATEGY

Nevertheless, the main goal of Zero-Trust architecture to be used in cloud environment is to protect the resources of cloud service provider (CSP) from successful data breaches. Furthermore, a clear understanding of CSP's data assets is critical for an effective implementation of Zero-Trust architecture. Following are the principles that lead to achieving Zero-Trust approach in cloud computing environment:

A. Identification of Sensitive Data in Cloud Service

This is the very basic principle towards achieving Zero-Trust approach. The CSP needs to identify the sensitive data such as, personally identifiable information, personal health information, intellectual property, or payment card data, etc. to determine the right security. Besides, this principle also endorses that the security configuration of cloud deployment ensures proper safety of the sensitive data.

B. Map Flows of Sensitive Sata in Cloud Service

This principle is about observing the flow of sensitive data across the cloud network. The flow may be multi-directional and

this principle results in creation of micro-networks due to the optimization of data flows.

C. End User Authorization (People)

Identity security and authentication of trusted users is principal to Zero-Trust approach. This includes the technologies such as Identity and Access Management (IAM), multi-factor authentication, etc. Therefore, all the access requests are continuously governed in order to monitor and validate the user trustworthiness.

D. Device Authorization

Trustworthiness of devices is most significant and foundational feature of a Zero-Trust scheme. Therefore, the devices connecting to cloud need to be evaluated using system of record solutions such as Device Managers.

E. Controlling Access

Zero-Trust security is characterized by least privilege access rights. Access control has amplified significance in cloud security. Further, the main cause of insider threats in cloud computing paradigm is overly excessive access leading to insider incidents.

F. Architect Zero-Trust Perimeters

This principle is more concerned about creating the micro-network or micro-perimeter. In Zero-Trust approach, a protect surface is identified. The protect surface is the network's most critical and valuable resources such as data, applications, services, etc. Therefore, with the protect surface identified in cloud system, traffic movement across the cloud is identified with respect to protect surface. This lets the cloud security leaders to understand who users are, what critical data they are using and how they are connecting in order to determine and enforce policy to ensure secure access to cloud resources. Once the flow of data, application, services, and infrastructure are known, optimal micro-network or micro-perimeter is created around it so that the best-fitting security is framed. In addition, the micro-perimeter can be created by deploying a segmentation gateway, also known as next-generation firewall to ensure only allowed legitimate traffic have access to protect surface. This step also considers using the physical or virtual security controls to implement the Zero-Trust micro-perimeters.

G. Application Security

Zero-Trust adoption agrees to secure and properly manage the application layer as well as containers and virtual machines. Multi-factor authentication (MFA) is considered as providing the proper access control to applications in Zero-Trust approach.

H. Monitor zero-trust ecosystem with security analytics

Embracing logs and data analytics in cloud environment would look for any malicious activity across the entire micro-perimeter ecosystem. Moreover, Zero-Trust leverages many different analytic system tools such as security user behavior analytics, advanced security analytics, etc. to facilitate cloud security experts to witness in real time what is happening and place defenses more intelligently.

I. Embrace security automation and orchestration

This step involves building the automation policies by applying security automation and orchestration tools. Zero-Trust scheme makes full use of security automation tools that automate tasks across cloud platform.

VI. ESTABLISHING TRUST IS FOUNDATIONAL

With emphasis on continuous monitoring and assessment for the application of Zero-Trust framework, an adaptive deployment model is however, essential. Threshold assigned by credentialing policies limit access by means of context-sensitive, dynamic extension. Besides, the process of determination of something (user, device, application, process, etc.) being trustworthy in this trust-centric shift is so difficult problem to begin countering with. Moreover, traditionally all the data and transactions are assumed to be trusted whereas device compromises, data breaches, and malicious activities contribute to degrade that trust. However, Zero-Trust strategy begins with an assumption that all the data and transactions are required to be deemed as untrusted from the inception. With this, a new problem gets countered as how to gain sufficient trust? Furthermore, based on the organizational requirements and key focuses, trust is bound to alter [19]. Therefore, to manage the trustworthiness of all transactions in an organization, Zero-Trust environment involves integration of control for data, users, devices and applications as shown in Figure 2.

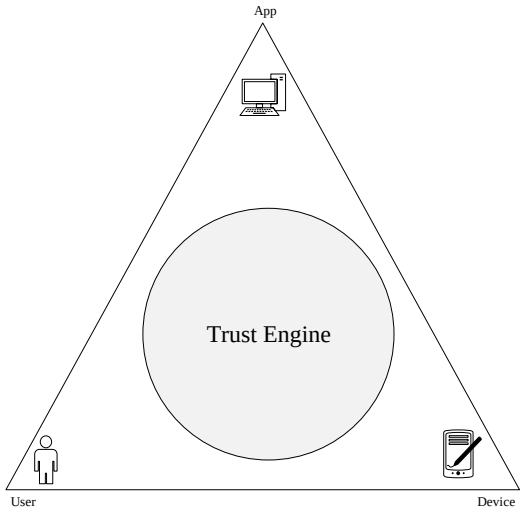

FIG. 2. ZERO-TRUST TRIANGLE

Trust Engine, dynamically computes the consolidated trust of a user, device, or application by giving it a trust score in a particular network. For every transaction request, the trust engine practices the evaluated trust score to make policy-based authorization conclusions.

Trust score governs the trustworthiness of a given user, application, or device. Its value is generated using different factors and conditions. Moreover, information like past interaction, experience with the system, access grants or denies by the system are examples of potential factors for determining the trust score.

Within the Zero-Trust Triangle, trust score is used by the Trust Engine to evaluate the trustworthiness of any user, device, or application that joins the network. The arrangement of data is questioned on demand in real-time to afford situational context to make the best authorization decisions possible.

VII. DISCUSSION

Security is perceived to be the most critical issue in cloud computing. As obtained from the exploration of previous sections, it is evident that trust plays an important role in cloud security. It enables the CSPs and customers to select the trustworthy entities in the heterogeneous cloud infrastructure. Trust in cloud environment is a promising topic of research which has been addressed in many academic publications. However, trust is not acquired, it is earned over time. Furthermore, trust can be used as a tool to deal with the security risk that is likely to increase as the use of cloud technology tends to increase. Moreover, a large number of trust models have been proposed by the research community. However, trust models require some properties to include quality of service parameters for effective trust establishment in cloud computing. Trust customization and trust aggregation challenges need to be accomplished for trust models. Besides, most of the trust models support subjective trust values. However, trust models usually support distributed computation for storing trust information.

Zero-Trust, indeed, is a modern technique to cybersecurity. Apparently, in the modern security environment, security schemes must be constructed around a zero-trust approach because the devices and external data sources from the multiple locations as there in internet of things (IoT) which implies, nothing inside or outside the network is trusted. Furthermore, with this conceptual model the complexities of the IT environment have been reduced to a larger extent. Therefore, embracing this model in cloud computing environment guarantees that the data and access across the network are secure and based on factors like location and user identity. Also, this model provides scope to inspect all cloud network traffic, monitors network patterns in order to keep track of every device and user connected to the cloud network at any given moment.

VIII. CONCLUSION

Cloud computing raises many challenges, but it also has implications on establishing trust. Though major cloud providers claim to offer strong protection, the goal to secure the cloud presence of users completely by the cloud providers happens to carry more chances to fail and thus, may lead to costly mistakes. Moreover, organizations find it difficult to keep tabs on the movement of data in the cloud and its access accordingly. Therefore, a conceptual model of zero trust strategy for cloud computing has been proposed and discussed in this study. The propounded trust strategy shall facilitate the CSPs and customers to choose trustworthy entities in cloud environment. It gives an efficient trust management benefits of cloud computing technology to both cloud provider and customer. As future work, the mathematical modeling with accurate details, proper formal languages and the relevant technology platform can be undertaken.

ACKNOWLEDGMENT

This work has been financial supported by Ministry of Electronics and Information Technology (MeitY), Government of India under its Visvesvaraya PhD scheme.

REFERENCES

[1]. Yuli Yang, Xinguang Peng, Donglai Fu, “A framework of cloud service selection based on trust mechanism”, Int. J. Ad Hoc and Ubiquitous Computing, Vol. 25, 2017.

[2]. Jingwei Huang, David M Nicol, “Trust mechanisms for cloud computing”, Journal of Cloud Computing: Advances, Systems and Applications 2013.

[3]. Alagumani Selvaraj, Subhashini Sundarajan, “Evidence-Based Trust Evaluation System for Cloud Services Using Fuzzy Logic”, International Journal of Fuzzy System, Springer, 2016.

[4]. Rajganesh Nagarajan, Ramkumar Thirunavukarasu, Selvamuthukumaran Shanmugam, “A Fuzzy-Based Intelligent Cloud Broker with MapReduce Framework to Evaluate the Trust Level of Cloud Services Using Customer Feedback”, Int. J. Fuzzy System, 2017.

[5]. Imad M. Abbadi, Andrew Martin, “Trust in the Cloud”, Elsevier, information security technical report, pp. 108-114, 2011.

[6]. Matin Chiregi, Nima Jafari Navimipour, “Cloud computing and trust evaluation: A systematic literature review of the state-of-the-art mechanisms”, Elsevier, Journal of Electrical Systems and Information Technology pp. 608–622, 2018.

[7]. Rizwana Shaikh, M. Sasikumar, “Trust Model for Measuring Security Strength of Cloud Computing Service”, Elsevier, International Conference on Advanced Computing Technologies and Applications (ICACTA), p. 380 – 389, 2015.

[8]. Albert S. Horvath III, Rajeev Agrawal, “Trust in Cloud Computing”, Proceedings of the IEEE Southeast Conference, 2015.

[9]. Archana B. Saxena, Meenu Dawe, “Trust Framework for IAAS—A Tool Based on Security Checks Through Standards and Certifications”, Information and Communication Technology for Intelligent Systems, Smart Innovation, Systems and Technologies, Springer Nature, 2019.

[10]. Pragati Prakash, Nidhi Ekka, Tanmay Kathane, Nishi Yadav, “Enhancement of Cloud Security and Strength of Service Using Trust Model”, Springer Nature ICICI, pp. 1345–1353, 2019.

[11]. Ritu, Sukhchandan Randhawa, Sushma Jain, “Trust Models in Cloud Computing: A Review”, I.J. Wireless and Microwave Technologies, p. 14-27, 2017.

[12]. Sheikh Mahbub Habib, Sascha Hauke, Sebastian Ries, Max Muhlhauser, “Trust as a facilitator in cloud computing: a survey”, Journal of Cloud Computing: Advances, Systems and Applications, 2012,

[13]. Matin Chiregi, Nima Jafari Navimipour, “A Comprehensive Study of the Trust Evaluation Mechanisms in the Cloud Computing”, Journal of Service Science Research, 2017.

[14]. Ashish Singh, Kakali Chatterjee, “A Mutual Trust Based Access Control Framework for Securing Electronic Healthcare System”, IEEE conference, 2017.

[15]. Xiaohui Li, Jingsha He, Bin Zhao, Jing Fang, Yixuan Zhang, Hongxing Liang, “A Method for Trust Quantification in Cloud Computing Environments”, International Journal of Distributed Sensor Networks-Hindawi, 2016.

[16]. Talal H. Noor, Quan Z. Sheng, “Trust as a Service: A Framework for Trust Management in Cloud Environments”, Springer, 2011.

[17]. Zhenguo Chen, Liqin Tian, Chuang Lin, “Trust evaluation model of cloud user based on behavior data”, International Journal of Distributed Sensor Networks, Vol. 14(5), 2018.

[18]. Evan Gilman and Doug Barth, “Zero Trust Networks, Building Secure Systems in Untrusted Networks”, Whitepaper, Publisher O’Reilly, 2017.

[19]. American Council for Technology-Industry Advisory Council, “Zero Trust Cybersecurity Current Trends” Whitepaper, 2019.