International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

http://TuEngr.com

PAPER ID: 10A17Q

A METHOD FOR ENSURING THE SECURE TRANSFER AND STORAGE OF BACKUP USER DATA AND INFORMATION FROM INTERNET OF THINGS DEVICES

Vladimir A. Kholopov [a*], Evgeny V. Kurnasov [a], Fedor V. Soklakov [a], Evgeny I. Korolev [b], Marina M. Untura [a], Roman G. Bolbakov [c]

[a] *Department of Industrial Informatics, Institute of Information Technologies, MIREA – Russian Technological University, RUSSIA.*
[b] *Department of Innovation Management, MIREA – Russian Technological University, RUSSIA.*
[c] *Department of Instrumental and Applied Software, Institute of Information Technologies, MIREA – Russian Technological University, RUSSIA.*

ARTICLEINFO

Article history:
Received 05 July 2019
Received in revised form 02 September 2019
Accepted 19 September 2019
Available online 30 September 2019

Keywords:
Information protection; Data backup; Data storage; Automation of data storage; Data synchronization; Data encryption; Cloud storage; Data security; User data protection; Digital Security; IoT.

ABSTRACT

This work is aimed at solving the problem of storage backup user data associated with security threats and risks of unauthorized information access to it, and with the possibility of destruction or damage to physical storage, as well as their theft in order to obtain stored data. The architecture of the proposed backup user data storage system is implemented on the platform of the user's operating system and consists of three main components – encryption, synchronization and data transfer to the cloud storage. The system architecture is also adapted to work with the Internet of Things (IoT) devices, which have recently been actively used and developed in various user and industrial systems. The information generated by these devices, in order to ensure the integrity and security of the entire system, is backed up in the data storage system, encrypted and transmitted to its physical or cloud storage.

1. INTRODUCTION

Currently, one of the most complex and critical areas of information security is the transfer and storage of user data with maintaining its integrity and security. According to Info-Watch, there were 213 leaks of confidential data in 2016 in Russia, which is 80% more than in 2015. Among this number of leaks, about 10% came from state and municipal authorities. Mainly, it is data related to payment information, as well as cash transfer operations documents. The leak of banking personal data is a critical factor for ordinary users.

A large number of users are registered on social networks, on various websites of digital

*Corresponding author (V. Kholopov). Tel: +7(903) 521-03-86 Email: holopov@gmail.com

distributors, such as Microsoft, Adobe, Autodesk, etc., where applications with a system of internal payments are widely used now. Such a large amount of credentials as logins and passwords is almost impossible to remember, so the problem of this data secure storage arisen.

Personal, official and scientific data: various documents, technical drawings, photos, videos and more stored in digital format are also valuable for users. When storing all these types of data on user devices, primarily on personal computers, it is necessary to ensure their secure storage. The function of ensuring the stored information security is almost completely implemented by specialized software packages – antiviruses. However, the data stored on computers remain vulnerable to theft or damage at the physical level even with good software protection. These vulnerabilities are related to the possibility of a hard disk theft, fire or other emergencies. Therefore, in addition to the above, it's necessary to further organize the secure storage and the backup user data transfer.

Yufeng Wang and Christian Hoffman (Wang and Tan, 2013; Hoffmann, *et al.*, 2015) describe in their works technologies for storing user data in the cloud in sufficient detail and note problems with the data secure storage in cloud services. In addition, the main encryption problem in (Hoffmann, *et al.*, 2015) is disclosed by the cloud provider, which increases the data theft risk or unauthorized decryption. Proposed by the authors' encryption solutions before sending data to the cloud are interesting for us, but the encryption and synchronization algorithms are implemented as a separate service and aren't capable to integrate with system processes.

Various backup strategies are considered in (Li, *et al.*, 2016; Kaur, *et al.*, 2018; Jung, *et al.*, 2017; Fernandes, *et al.*, 2014). It is necessary to ensure the data duplication absence for optimal processing of the data backup system. For example, the problem of duplicate data storage in the cloud and the possibility of its recovery without the user decision is solved in Lai's J. work (Lai, *et al.*, 2017). Various methods and algorithms used in the process of data deduplication are considered in (Bhalerao and Pawar, 2017).

The majority of the proposed solutions for the secure synchronization and storage of backup data using cloud services don't ensure data encryption services and the ability to store them on the client-side. It leads to the possibility of unauthorized access to user data during its transfer or storage. Thus, the most preferred solution would be a tool used reliable and verifiable client-side encryption which is able to work on their own infrastructure.

In this paper, we will consider an integrated approach for organizing a system for secure transfer and storage backup data on the user's end device and in the cloud.

2. ANALYSIS OF SOFTWARE PRODUCTS FOR SECURE DATA STORAGE

For secure storage of valuable data for a user, including backup, ready-made solutions exist. Acronis True Image is one of the examples of such solutions and allows us to store 1 TB of data in the cloud for a user. Its functionality includes full backup of the system disk, the ability to clone an active disk, including the operating system, system files and settings. Data encryption is performed using the AES-256 standard and it's possible to add electronic signatures for verifying of files authenticity. Another good example is an application WISeID Kaspersky Lab Security created by Kaspersky Lab with WISeID together. This solution provides 3 GB of secure storage for user personal data with the synchronization option of various user devices. For added protection, the system uses face recognition as a user authentication method. Having considered the main market decisions, it can be noted that systems of this class certainly fulfill to varying degrees the assigned task of ensuring safety

for backup user data storage. However, it's worth mentioning that these systems operating based on a paid license: $ 20 is paid for Kaspersky Lab Security's WISeID application annual license, $ 40 – $ 50 per year – for Acronis's solution for one workstation and $190–$300 per year for one server. These products are developed primarily for OS Windows and MacOS, as well as for mobile platforms iOS and Android. Also, it should be noted, that although these products provide an excellent service for protecting information on the cloud side, they still don't provide the required protection against theft and further reading of the hard drives of the users themselves.

3. THE ARCHITECTURE AND OPERATING ALGORITHM OF THE PROPOSED SYSTEM FOR ENSURING THE SECURE TRANSFER AND STORAGE OF BACKUP DATA

To ensure the secure transfer and storage of backup data on the user's end device, as well as in cloud storage, it is necessary to solve the problems associated with designing the most efficient data encryption and synchronization system architecture, selecting the necessary tools, configuring and organizing the storage of software components in the file system and maximum automation of their work. It is also advisable to analyze the main indicators of data security of the protected object (Magomedov, 2017).

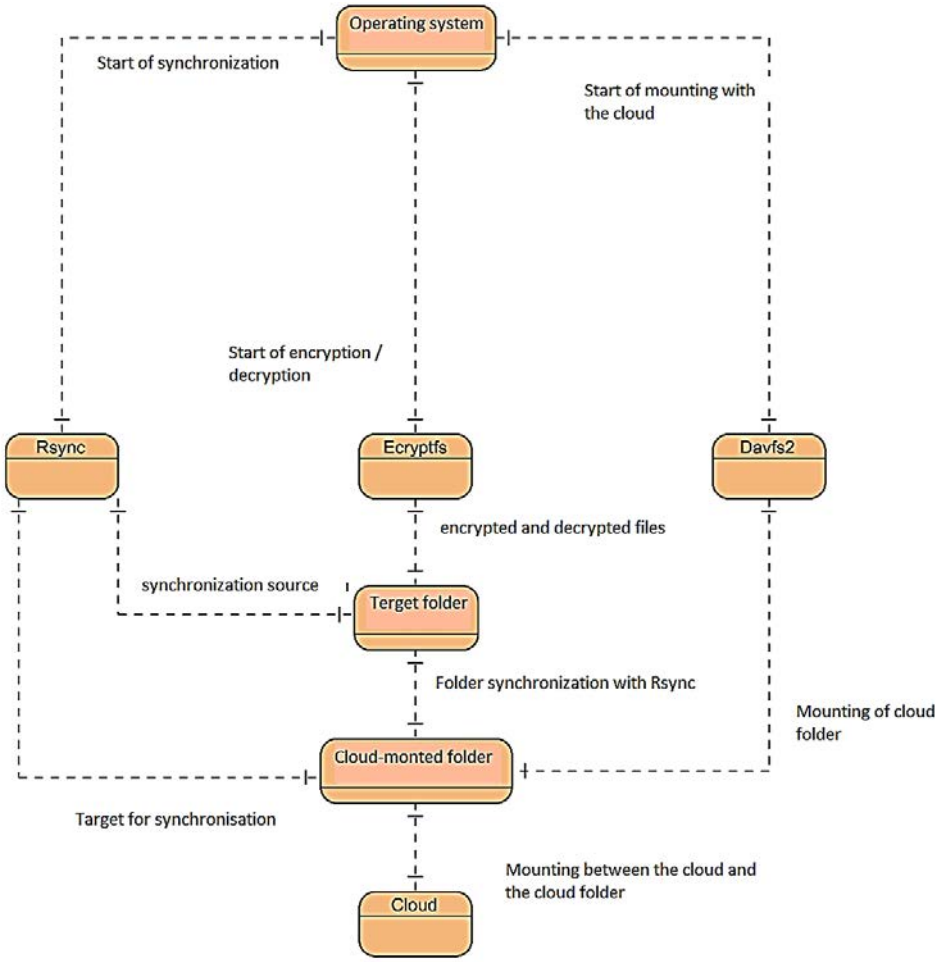

Figure 1: The ER-diagram of security systems for storage and transfer backup data.

The basis of the proposed method for ensuring the security of storage and transfer of backup user data is a set of standard operating system components. These components are shown in the form

*Corresponding author (V. Kholopov). Tel: +7(903) 521-03-86 Email: holopov@gmail.com Volume 10 No.17 ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8 Paper ID: 10A17Q http://TUENGR.COM/V10A/10A17Q.pdf DOI: 10.14456/ITJEMAST.2019.243

entities, which are abstractions of the real components of the operating system and itself both, as depicted on the ER-diagram (Figure 1):

- Operating System – an operating system that interacts with encryption, synchronization, and data transfer utilities to the cloud, namely, it gives commands to start the execution of these processes;
- Target Folder – is the user target directory where a user can transfer the secured data;
- Cloud Mounted Folder – is a directory in the cloud that mounts to the user's file system using the Webdav utility. Encrypted files in this directory are synchronized with the target directory of the user Target Folder using the Rsync utility;
- Cloud – is cloud structure that stores encrypted backup data on the Internet;
- Ecrypfs, Rsync, Webdav – are entities of operating system utilities for encryption, synchronization and data transfer.

The relationships between these entities in the diagram reflect all the processes within and between them, as well as the transferred data.

The algorithm of the system during encryption and synchronization processes of user data is depicted in Figure 2.

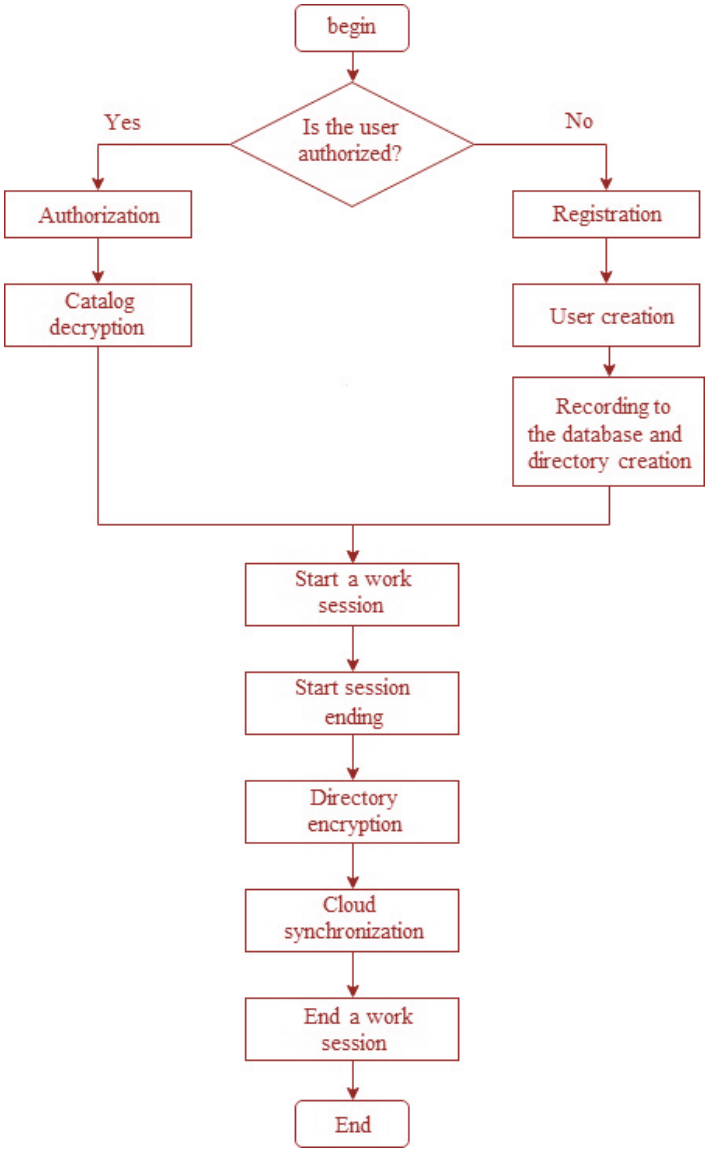

Figure 2: The algorithm of the system at encryption and synchronization of the user data process.

After a successful user authorization procedure in the operating system, a special directory is allocated for the user where he places files that need to be secured. Next, a directory from the cloud is

mounted on the user's file system. After the end of work (end a user's session in the operating system) and turning off the user's device the mounted directory and the directory on the end device are encrypted and then synchronized. Thus, the mounted folder is unmounted from the user's file system after the ended session and remains in the cloud, providing independent storage of backup data in several storages.

This solution improvement was carried out in the Linux mint operating system using the following tools:

- Ecrypyfs – is the utility allowing you to encrypt user-selected data with any of eight encryption algorithms with a choice of key lengths. Ecryptfs functions are powerful and flexible, which allows them to be used automatically;
- Rsync – is a tool that allows you to quite simply and reliably synchronize data between directories in the file system of the user's end device and between devices both over a local network using an ssh-channel;
- davfs2 – is a program that allows mounting directories located in the cloud with the file system of the end device using the Webdav http protocol extension.

These tools, determined above, have good functionality and flexibility and they are easy to use, but they don't have a graphical interface. We developed scenarios of its relations to automate the work of all programs. At the same time, the davfs2 utility commands weren't included in the scripts, since they're run only in privileged mode, which isn't able to provide fully automated system operating mode.

4. IMPLEMENTATION OF THE SYSTEM FOR SECURE STORAGE AND TRANSFER BACKUP DATA

4.1 COMPONENTS SETUP

As a rule, the majority of the programs necessary for implementing the system are already installed in distributions of the Linux operating system. The remaining components can be installed from the terminal emulator with the command: *sudo apt-get install <Program-Name>*. The installation of some programs requires privileged rights, and therefore, you can use the *sudo* utility, which provides program execution with administrator rights.

- The ecryptfs utility is configured as follows: first, a directory for encryption is selected, then it is mounted with a selected password for encryption. Next, you need to choose an encryption method (ecryptfs supports six different algorithms, the most popular of which is aes), the key size is specified in bytes. At this step the main configuration of the utility is considered complete;
- For convenient work with the davfs2 program that transfers data to the cloud, you need to create a directory that will act as a mount point with the cloud (you can use ready-made cloud services). After that the created directory is linked to the repository using the authentication data in the service used (login and password);
- The Rsync utility works after installation without preliminary settings, because davfs2 is used to transfer data. At the same time, existing services are used to store data in the cloud, and there isn't necessary to configure a Rsync-server.

4.2 FILE SYSTEM ARCHITECTURE

It is necessary to store system's components (utilities and scripts) in defined directories of the file system for the system operating:

*Corresponding author (V. Kholopov). Tel: +7(903) 521-03-86 Email: holopov@gmail.com Volume 10 No.17 ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8 Paper ID: 10A17Q http://TUENGR.COM/V10A/10A17Q.pdf DOI: 10.14456/ITJEMAST.2019.243

- /home/users – is a directory address with protected user data on the working machine;
- /home/users / Documents – is a directory address for mount point with the cloud;
- / etc – is a directory address for storage Rsync synchronization utilities and creating a mount point with davfs2 cloud;
- / usr/sbin – is a directory address of the script for creating the mount point and data decryption at the authorization process in the system;
- / etc / rc0 – is a storage address of the script for data encryption and synchronization with the cloud when the working machine is turned off.

The ecryptfs utility is located in the directory address with protected data at the stage of system configuration.

To ensure the integrity of the davfs2 and Rsync components, they must be located in directories that require administrator rights.

4.3 SCENARIOS FOR SYSTEM OPERATING AUTOMATION

The work with secured files can be optimized by scripts development that will automatically run when a user logs into their operating system profile.

For example, data decryption using the built-in Ecryptfs utility can be implemented with the script:

```
#bin/bash
ecryptfs-add-passphrase
mount –i /home/user/name_of_folder
```

The data encryption and synchronization with the cloud can be implemented with the scenario.

```
#bin/bash
umount /home/user/name_of_folder
rsync –azv /home/user/name_of_folder
home/user/Documents/name_of_folder
```

These scripts are implemented in Bash-Script programming language.

As noted earlier, cloud-mount point creation commands weren't included in the script, because these commands are executed only if the user has administrator rights.

4.4 INTEGRATION WITH IOT SYSTEMS

Intelligent devices with Internet of Things (IoT) technology supported network functions form now a whole new set of functions and capabilities in the field of security, analytics and management (Morin and Nemova, 2017; Kazykhanov and Rednikov, 2017; Balaji, *et al*., 2019).

As rule, the basis of the Internet of things device usually consists of three main components: data acquisition using built-in sensors, communication between each other using special protocols (for example, MQTT) and data transferring. Thus, it becomes relevant to resolve issues of ensuring the secure and reliable storage organization of backup data transferred from IoT-devices.

The architecture of the proposed system allows ensuring the reliable backup storage of user data, as well as data from IoT-devices and smart home control systems.

In all cases, it is obvious that user data has great value, for example, if you enter the residential or industrial room using electronic card locks or fingerprints. The development of cyberphysical

systems, digital production technologies and the digital twins (Seiger, *et al.*, 2019; Leng, *et al.*, 2019; Zheng, *et al.*, 2018; Nof and Silva, 2018; Kholopov, *et al.*, *2018*; Kashirskaya, *et al.*, 2017; Kholopov, *et al.*, 2019) concept made information integrity concept very important generalizing indicator of systems' effectiveness to provide relevant information on the current and predicted state of the system. Any unauthorized violation of the stored data can lead to inappropriate behavior of the entire system or increase the data processing time, which is critical for real-time systems. For these reasons, the proposed system should have a minimum interaction time with IoT-devices – only in order to obtain the required amount of data for further transfer, encryption and storage on local hard drives and in cloud storage.

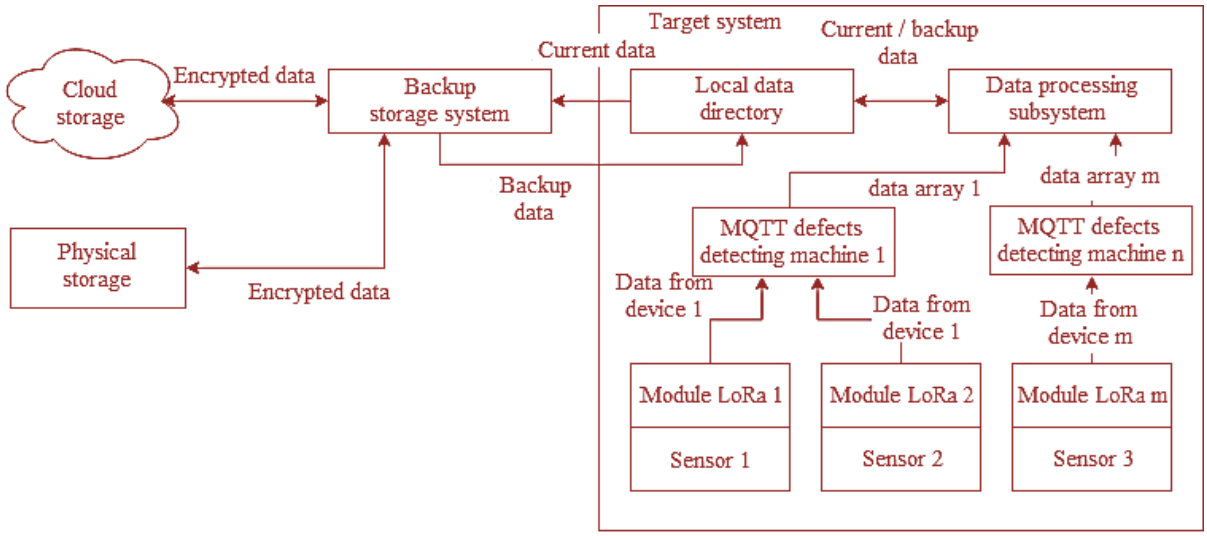

Figure 3: Architectural Integration with IoT.

In this regard, a separation architecture is proposed assumed that the target system and the backup data storage system of the common information space operating separately, when the first system serves as a data generator and the second – as a data consumer or as an emergency situations generator. Figure 3 depicted the structural diagram of the proposed solution, which has all the necessary elements of integration with IoT-systems.

Data is generated in the target system using sensors and is transmitted to the MQTT defects detecting machine using LoRa modules (Augustin, *et al.*, 2016), which acts as a local data collector, to provide them to the data processing subsystem already. LoRa modules are a good solution but there is another because of the presence of the interaction network in the IoT-systems which can be based on ZigBee mesh networks. These networks have better data transfer speed and worse touch area according to the radius value than LoRa networks. In addition to interacting with other subsystems, the information processing subsystem interacts with the local data directory. The directory in simple systems can be an ordinary directory, but in more complex systems it can be a separate device with a file system (for example, a storage server or network storage). The data processing subsystem in normal mode copies the received data into this directory at certain intervals, after which the backup storage system collects this data, encrypts it and sends it to its physical and cloud storage. When it is necessary to read the backup data at emergency events, the data processing subsystem makes a request to the data storage system, after which data from the physical storage is provided, but if the

*Corresponding author (V. Kholopov). Tel: +7(903) 521-03-86 Email: holopov@gmail.com

physical storage is disabled, data is provided from the cloud storage.

5. DISCUSSION

One of the most priority areas is the protection of information in the field of information technology, the protection and secure transfer of backup user data in particular. Despite the fact that the user data offline storage is more secure, we can't deny the fact that we live in a connected world where data is periodically transmitted or posted on the Internet.

6. CONCLUSION

To organize safe and reliable storage of backup user data, a working prototype of the system, which reduces the theoretical frequency of losing user data was created and approved.

This system is a console program with the partially automated operation of the majority processes, allowing you to fully complete all tasks. The system architecture makes it possible to use a graphical interface, as well as the ability to integrate with other cloud services, such as Dropbox, Yandex-drive, Google-drive. Unlike commercial solutions, the proposed system can be freely distributed, which is important for small networks and individual users.

The considered method of the store and transferring backup user data performs encryption on the user side, which ensures more transparent information protection.

The system architecture is adapted to work with IoT-devices and can be considered as simple and at the same time an effective solution for collecting and providing backup data to the system. It's assumed that for greater reliability, the target IoT-system will also be equipped with data storage systems, which will increase the ability to preserve the information integrity in the proposed system together.

7. DATA AND MATERIAL AVAILABILITY

This article already includes all the information about this study.

8. ACKNOWLEDGEMENT

Financial support was provided by MIREA Russian Technological University as part of the ITsMR-12 research initiative regarding information-based control systems for the assembly of complex products.

9. REFERENCES

Augustin, Aloÿs, Y. Jiazi, T. Clausen, and William M. Townsley. (2016). A Study of LoRa: Long Range & Low Power Networks for the Internet of Things. *Sensors*, 16(9), 1-18.

Balaji, S., K. Nathani, and R. Santhakumar. (2019). IoT Technology, Applications and Challenges: A Contemporary Survey. *Wireless Personal Communications*, 108(1), 363-388.

Bhalerao, Anand R. and A. Pawar. (2017). A survey: On data deduplication for efficiently utilizing cloud storage for big data backups. *2017 International Conference on Trends in Electronics and Informatics (ICEI)*, 933-938.

Fernandes, Diogo A.B., Liliana F.B. Soares, João V. Gomes, Mário M. Freire, and Pedro R.M.

Inácio. (2014). Security issues in cloud environments: a survey. *International Journal of Information Security (IJIS)*, 13(2), 113-170.

Hoffmann, C., C. Brand, and S. Heinzl. (2015). Towards an Architecture for End-to-End-Encrypted File Synchronization Systems. *24th IEEE International Conference on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE)*, 170-175.

Jung, H., Y. Park, CW. Song, and S. Kang. (2017). PCS: a parity-based personal data recovery service in cloud. *Cluster Computing*, 20(3), 2655-2668.

Kashirskaya, Elizaveta N., Evgeny V. Kurnasov, Vladimir A. Kholopov, and Anna G. Shmeleva. (2017). Methodology for assessing the implementation of the production process. *2017 IEEE 2nd International Conference on Control in Technical Systems (CTS)*, 232-235.

Kaur, R., I. Chana, and J. Bhattacharya. (2018). Data deduplication techniques for efficient cloud storage management: a systematic review. *The Journal of Supercomputing*, 74(5), 2035-2085.

Kazykhanov, A.A. and D.V. Rednikov. (2017). The proliferation of IoT as a positive factor in the development of society. *Alleya nauki (Science Alley)*, 2(11), 478-480.

Kholopov, Vladimir A., Elizaveta N. Kashirskaya, Alexander P. Kushnir, Evgeny V. Kurnasov, Alexander V. Ragutkin, and V. V. Pirogov. (2018). Development of Digital Machine-Building Production in the Industry 4.0 Concept. *Journal of Machinery Manufacture and Reliability*, 47(4), 380-385.

Kholopov, Vladimir A., Elizaveta N. Kashirskaya, Anna G. Shmeleva, and Evgeny.V. Kurnasov. (2019). An Intelligent Monitoring System for Execution of Machine Engineering Processes. *Journal of Machinery Manufacture and Reliability*, 48(5), 464-475.

Lai, J., J. Xiong, C. Wang, G. Wu, and Y. Li. (2017). A Secure Cloud Backup System with Deduplication and Assured Deletion. *11th International Conference on Provable Security*, LNCS 10592, 74-83.

Leng, J., H. Zhang, D. Yan, Q. Liu, X. Chen, and D. Zhang. (2019). Digital twin-driven manufacturing cyber-physical system for parallel controlling of smart workshop. *Journal of Ambient Intelligence and Humanized Computing*, 10(3), 1155-1166.

Li, M., C. Qin, J. Li, and Patrick P. C. Lee. (2016). CDStore: Toward Reliable, Secure, and Cost-Efficient Cloud Storage via Convergent Dispersal. *IEEE Internet Computing*, 20(3), 45-53.

Magomedov, Sh.G. (2017). Assessment of the impact of confounding factors in the performance information security. *Rossiyskiy tekhnologicheskiy zhurnal (Russian technological journal)*, 5(2(16)), 47-56.

Morin, Kevin and U. Nemova. (2017). Successful Mastery of IoT: it is Necessary to Consider in Addition to the Technology. *Promyshlennye ASU i kontrollery (Industrial ACS and controllers)*, No.3, 35-37.

Nof, Shimon Y. and Jose R. Silva. (2018). Perspectives on Manufacturing Automation Under the Digital and Cyber Convergence. *Polytechnica*, 1(1-2), 36-47.

Seiger, R., S. Huber, P. Heisig, and U. Aßmann. (2019). Toward a framework for self-adaptive workflows in cyber-physical systems. *Software & Systems Modeling*, 18(2), 1117-1134.

Wang, Yufeng and Chiu C. Tan. (2013). Looking at the overheads of transmitting encrypted data to the cloud. *2013 IEEE Conference on Communications and Network Security (CNS)*, 493-497.

*Corresponding author (V. Kholopov). Tel: +7(903) 521-03-86 Email: holopov@gmail.com Volume 10 No.17 ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8 Paper ID: 10A17Q http://TUENGR.COM/V10A/10A17Q.pdf DOI: 10.14456/ITJEMAST.2019.243

Zheng, P., H. Wang, Z. Sang, Ray Y. Zhong, Y. Liu, C. Liu, K. Mubarok, S. Yu, and X. Xu. (2018). Smart manufacturing systems for Industry 4.0: Conceptual framework, scenarios, and future perspectives. *Frontiers of Mechanical Engineering*, 13(2), 137-150.

Dr.Vladimir A. Kholopov, Ph.D. (Engineering), is Head of the Industrial Informatics Department of Institute of Information Technologies, MIREA – Russian Technological University, Moscow, Russia. He is interested in Automation of Technological Processes, Control, and Production, Information Systems Design, Real-Time Computing Systems, Integrated Design and Management Systems, Integrated Safety of Production Systems, Digital Devices, Automatic Programming of Control Systems.

Dr.Evgeny V. Kurnasov, Ph.D. (Engineering), is an Associate Professor of the Industrial Informatics Department of Institute of Information Technologies, MIREA – Russian Technological University, Moscow, Russia. He is interested in Digital Devices, Automation and Control Tools, Integrated Design and Management Systems, Programming in Control and Automation Systems, Automation of Designing Systems and Controls.

Fedor V. Soklakov is a Master's of Engineering degree student of the Industrial Informatics Department of Institute of Information Technologies, MIREA – Russian Technological University, Moscow, Russia. He is interested in Digital Securities.

Dr.Evgeny I. Korolev is Head of the Department of Integrated Innovation Projects and Programm of the Institute of Innovation Management, MIREA – Russian Technological University, Moscow, Russia. He is interested in Innovation Projects and Innovation Management.

Marina M. Untura is a Laboratory Assistant of the Industrial Informatics Department of Institute of Information Technologies, MIREA – Russian Technological University, Moscow, Russia.

Dr.Roman G. Bolbakov, Ph.D. (Engineering), is an Associate Professor of the Instrumental and Applied Software Department of Institute of Information Technologies, MIREA – Russian Technological University, Moscow, Russia). He is interested in Software Security and Encription.