ANNOTATION
dissertation work Temirbekova Zhanerke Erlanovna on the topic "Using AtmelAVR microcontrollers to ensure the security of computing clusters and systems", submitted for the degree of Doctor of Philosophy (PhD) in the specialty "6D070400-Computer Engineering and Software"

The relevance of the work. Every sector, from healthcare to manufacturing, uses IoT (Internet of Things) devices. The main purpose of IoT technology is to allow connected devices to communicate with each other, exchange data, store data and perform calculations in accordance with the requirements of the user.

One of the varieties of IoT is the Internet of Medical Things (IoMT) is a growing field of healthcare and one of the specialized uses of IoT, which includes the use of connected medical devices for remote monitoring, data collection and analysis. Atmel AVR microcontrollers are widely used in IoMT devices due to their low power consumption, high performance and reliability. Here are some examples of IoMT devices using Atmel AVR microcontrollers:

1. Wearable health monitors;
2. Intelligent insulin pens;
3. Connected inhalers;
4. Systems for remote monitoring of patients;
5. Smart pill bottles;
6. Telemedicine devices.

By 2024, the total number of IoT devices predicted to reach 83 billion. Obviously, without proper security measures, any connected IoT device is vulnerable to hacking, loss of functionality or user data. According to a 2022 Palo Alto Networks report, 98% of all IoT device traffic is unencrypted, indicating that private and sensitive data on the network not kept secret and allows attackers to eavesdrop on unencrypted network traffic, collect personal or sensitive information, and then use this information for your own purposes. According to SAM Seamless Network, there were over 1.5 billion attacks against IoT devices in 2021, nearly 900 million of which were IoT-related phishing attacks.

IoT devices themselves are not analogous to computers, they cannot perform any resource-intensive task from start to finish, and they perform only other IoT devices modify some part of it and the rest of the parts. In other words, IoTs work in a certain group or cluster they jointly solve some problem. The information transmitted between them must encrypted in order to protect it, but on the other hand, so that we do not violate the overall result of the work and be able to perform operations on this data, it should be possible to perform actions on encrypted individual data packets as if they were in unencrypted form. This feature is provided by homomorphic encryption, which can be implemented in AtmelAVR microcontrollers (DFRobot Beetle BLUE, Atmega 328, Atmega 32u4, Atmega 2560) that control IoT devices in medicine, consumer electronics and manufacturing.

In recent years, more and more works have appeared in the world related to FHE (fully homomorphic encryption) for IoT devices. Sujoy S.R., Goyuri P., Deepika N. show that homomorphic encryption algorithms can be applied to IoT applications and devices, and also aim to increase computing speed while maintaining data privacy.

Goran D., Milan M., Pavle V. in the work "Evaluation of the implementation of homomorphic encryption in an IoT device" evaluated the features of the BFV and BGV homomorphic encryption mechanisms and measured their performance. The paper evaluated encryption schemes on an IoT platform based on the Raspberry Pi 4 model, which show that homomorphic encryption operations can be applied on embedded devices and are primarily aimed at improving privacy and providing higher throughput and lower latency to accelerate more applications FHE.

Among the representatives of the Russian scientific community, the works of the following scientists can distinguished: I.B. Saenko, V.A. Desnitsky (Moscow), I.V. Kotenko (Yekaterinburg), P.D. Zegda (St. Petersburg).

Scientists of the Institute of Information and Computing Technologies Committee of Science of the Ministry of Education and Science RK: Biyashev R.G., Nysanbayeva S.E., Kapalova N.A., Kunbolat A.

Based on the foregoing, we can conclude that the use of effective algorithms, methods and software for the security of IoT devices and applications is very relevant. AtmelAVR microcontrollers can used very effectively in a wide range of IoMT applications to collect and transmit real-time data, allowing healthcare professionals to make informed decisions about the health of their patients.

The purpose of the dissertation research: To develop and implement a fully homomorphic encryption library architecture that allows you to perform all arithmetic operations on encrypted data on a group of AtmelAVR microcontrollers for secure storage and protection of information transfer between IoT devices.

The objectives of the research, realizing the purpose of the dissertation work:

1. Analysis of data protection methods and devices in a cluster of IoT devices.

2. Improvement of the homomorphic encryption algorithm used in the AtmelAVR microcontroller.

3. Development of the library architecture in the AtmelAVR microcontroller (DFRobot Beetle BLUE, Atmega 328, Atmega 32u4, Atmega 2560, ESP 32) to ensure the security of a cluster of IoT devices.

4. Evaluation of the quality of the library on the AtmelAVR microcontroller, as well as a comparison of its performance with the performance of other well-known libraries.

Object of research. Secure data transfer between IoT devices.

Subject of research. Ways to protect data using a microcontroller.

Research methods. Methods for processing information in a microcontroller, methods for analyzing and evaluating the effectiveness of using microcontrollers to protect IoT clusters, a method of homomorphic encryption.

Scientific novelty:

The scientific novelty of the work lies in the fact that for the first time the architecture of the library of homomorphic encryption algorithms was developed and implemented on AtmelAVR microcontrollers (DFRobot Beetle BLUE, Atmega 328, Atmega 32u4, Atmega 2560, ESP 32) to protect data transmission in a group of IoMT devices, in order to in order, without violating the confidentiality of the transmitted information, to ensure the joint operation of IoMT devices to process this data, as if it were in unencrypted form. In the course of experiments to evaluate the performance of the developed library and known algorithms for homomorphic encryption, Krendelev S.F. and Abramov A., the library proposed in the dissertation work showed ease of connection and use, as well as data calculation speed about 1.52 times higher.

The theoretical significance of the work.

Improvement and adaptation for microcontrollers and data processing processes on IoMT devices of fully homomorphic encryption algorithms that allow you to work with integers and perform all arithmetic operations on them.

The practical significance of the work. Development of the architecture of the library for the microcontroller and establishment of the scheme, methodology and order of data exchange between the modules and methods of the library in order to optimize its work.

Basic provisions for defense.

The architecture of a library of homomorphic encryption algorithms for protecting transmitted data in a system of IoMT devices, developed and implemented on a group of AtmelAVR microcontrollers, which during the study were supplemented with an SD card, an SD module and a programmer to expand the possibilities of working with different data structures, is presented for protection.

Level of reliability and results of approbation. The scientific results of the work presented and discussed at the following international scientific conferences and scientific seminars:

1) XLI, XLII International scientific and practical conference «Innovative technologies in transport: knowledge, science, experience»;

2) International scientific and practical conference «Actual and perspective directions of development of scientific and technological progress»;

4) International Research Conference on Technology, Science, Engineering and Economy held Seattle, USA;

5) VI international scientific and practical conference «Physics - the role of mathematical sciences in the modern educational space»;

6) The 5th International Conference on Energy, Environmental and Information System (ICENIS 2020), Semarang, Indonesia //E3S Web of Conferences.

In addition, this topic discussed repeatedly at the Department of Computer Science of the Kazakh National University named after al-Farabi and at scientific seminars of the Faculty of Information Technology, as well as at the Institute of Information and Computing Technologies of the Ministry of Education and Science of the Republic of Kazakhstan.

Contribution of the doctoral student to the preparation of each publication. Published articles and scientific papers describe the results of research on the topic of the dissertation. During the scientific work, 12 scientific papers were written and 1 author's certificate was received, including: 2 scientific articles in a journal indexed in the Scopus database:

1. Pyrkova A.Yu., Temirbekova Zh.E. “Compare encryption performance across devices to ensure the security of the IoT”, Indonesian Journal of Electrical Engineering and Computer Science, -2020. -Vol. 20.-No. 2. - P. 894-902. (Scopus percentile - 45). Q3

2. Temirbekova Zh.E., Pyrkova A.Yu. “Improving teachers’ skills to integrate the microcontroller technology in computer engineering education”, Education and information technology, -2022 doi: 10.1007/s10639-021-10875-8 (Scopus percentile - 95). Q1

Three articles in journals recommended by the Committee for Control in the Sphere of Education and Science of the Ministry of Education and Science of the Republic of Kazakhstan:

1. Temirbekova Zh.E., B.K. Alymbayeva. “Using Atmel AVR microcontrollers for safety-performance computing” // Bulletin of KazNITU, -2017. No. 2, - P. 192 - 195

2. Pyrkova A.Yu., Temirbekova Zh.E. “Possibilities of using a BLE Nano Kit microcontroller to develop cryptographic libraries” // Bulletin of KazNITU, - 2018. No. 2, - P. 477 - 481

3. Pyrkova A.Yu., Temirbekova Zh.E. “Performing symmetric encryption mbed platform” // Bulletin of KazNITU, - 2018. No. 2, - P. 473 - 476

In the collections of international scientific and practical conferences indexed in the Scopus database, 2 scientific articles have been published:

1. Temirbekova Zh.E., Pyrkova A.Yu. “Using FHE in a binary ring Encryption and Decryption with BLE Nano kit microcontroller” //E3S Web of Conferences 202 (ICENIS 2020), -2020. 15002

2. Temirbekova Zh.E., Pyrkova A.Yu., Abdiakhmetova Zh. “Library of fully homomorphic encryption on a microcontroller” //2022 International Conference on Smart Information Systems and Technologies 28-30 April, 2022, Nur-Sultan, doi:10.1109/SIST54437.2022.9945722.

Five scientific articles published in the collections of international scientific conferences:

1. Temirbekova Zh.E "Programming microcontroller AVR Atmega8" // Proceedings of the XLI International scientific and practical conference "Innovative technologies in transport: knowledge, science, practice", April 3-4, 2017, Almaty, Kazakhstan, (Volume I), p. 102 -104.

2. Pyrkova A.Yu, Temirbekova Zh.E "Use homomorphic encryption for data security" // Proceedings of the XLII International scientific and practical conference "Innovative technologies in transport: knowledge, science, practice", 2018, Almaty, Kazakhstan, (Volume I), p. 83-85.

3. Temirbekova Zh.E “For data security symmetric encryption algorithm” // International scientific-practical conference “Actual and promising directions for the development of scientific and technological progress”, January 30, 2020, Russia, Kemerovo, p. 26-30

4. Pyrkova A.Yu, Temirbekova Zh.E. “Using microcontrollers to ensure data security”, International Research Conference on Technology, Science, Engineering and Economy held Seattle, USA, February 28th, 2020, p. 52-60

5. Temirbekova Zh.E. "Library of the complete homomorphic encryption algorithm" Proceedings of the 6th international scientific-practical conference "Physics - the role of mathematical sciences in the modern educational space", December 7, 2021, Atyrau, Kazakhstan, p. 326-331.

Volume and structure of the work. The total volume of work is 92 pages. The dissertation consists of an introduction, 4 sections, a conclusion, a list of used sources from 104 names, 2 appendices, includes 46 figures and 17 tables.

In the introduction, the relevance of the chosen topic of the dissertation work, the goal, object, subject and tasks of the research discussed. The obtained results of the conducted studies, their scientific novelty and practical significance described.

The first section is devoted to the analysis of various architectures of AtmelAVR microcontrollers. The terms and concepts used in the dissertation work presented. The reliability of various AtmelAVR microcontrollers is calculated, and the microcontroller used in the dissertation is determined based on this. Experimental calculations for various cryptosystems of homomorphic encryption performed on the AtmelAVR microcontroller. Effective algorithms of homomorphic encryption on a microcontroller shown based on experimental calculations. Here are some references and reviews of scientific works on this topic.

In the second section, the process of modification of homomorphic encryption methods is described: in the algorithm of S.F. Krendeleva added subtraction and division operations to algorithm A. Abramova added the subtraction operation. The improved fully homomorphic encryption presented in the form of a block diagram.

The third section presents the architecture of the fully homomorphic encryption library for the AtmelAVR microcontroller. The studied scheme of connection of the built-in library to the microcontroller. The improved encryption algorithm explained based on a block diagram (key generation, encryption, homomorphic transformation and decryption). The main system requirements of the software, explanations of the operation shown.

The fourth section describes performance testing of the library, built because of the proposed architecture, on the AtmelAVR microcontroller. The results presented in the form of a diagram. The developed library compared with the works of other authors, and the results of research show that the improved completely homomorphic encryption presented in the thesis works about 1.52 times faster.

In conclusion, the conclusion of this dissertation work presented.