Securing Data Transmission for Radiation Monitoring System in Nuclear Installation

Nanang Triagung Edi H.
Departement of Computer Science and Electronics, Gadjah Mada University, Yogyakarta, Indonesia

Edi Winarko
Departement of Computer Science and Electronics, Gadjah Mada University, Yogyakarta, Indonesia

Ahmad Ashari
Departement of Computer Science and Electronics, Gadjah Mada University, Yogyakarta, Indonesia

ABSTRACT
Radiation exposure or radioactive release from nuclear installation should be monitored for ensuring safety and security to the worker, member of the public, and the environment. Radiological Data Monitoring System (RDMS) is one of the systems for conducting radiation monitoring. Transfer data process from local RDMS to central server generates some cyber vulnerabilities, including data confidentiality, integrity, and availability. A literature study to propose secure data transmission for supporting radiation monitoring system in nuclear installation has been conducted. For ensuring secure data transmission, some data security mechanism should be implemented, such as authentication process for each new RDMS, encryption of data uplink and downlink. Both symmetric and asymmetric cryptography algorithm can be implemented. Combination of algorithm cryptography, such as Advanced Encryption Standard (AES) and Elliptical Curve Cryptography (ECC), or Asymmetric key based Cryptographic Algorithm using Four Prime numbers (ACAFP) and ECC will be powerful for increasing the data security level in the data transmission process. In the development of security protocol algorithm, it should be considered the system configuration, capability of the local microprocessor, and power supply capacity in RDMS.

General Terms
Data Transmission Security, Protocol Algorithms

Keywords
secure data transmission, radiation monitoring, nuclear installation, cryptography.

1. INTRODUCTION
Operation of nuclear installation always involves radioactive material, included nuclear material. In this activity, the possibility of radioactive discharge or release from the installation to the environment happens, both under normal condition, especially in the event of incident or accident. To ensure that radioactive discharged or released does not exceed specified safety limits, it should be monitored routinely by implementing radiation monitoring system. Radiation monitoring system should be conducted inside of and until some specified radius outside from the installation (IAEA, 2005).

Radiation monitoring system has the main function to determine safety status or condition of the nuclear installation. If the monitoring data shows that radiation level below the specified safety limits, the operation condition is normal. Otherwise, if the monitoring data shows that radiation level exceeds the specified safety limits, it can be said that there has been a radiation incident or accident. In the second condition, the monitoring data acts as an early warning system. It becomes a reference safety limit to control and establish countermeasure actions based on specified emergency preparedness procedure.

Besides implemented for radiation discharge or release monitoring from a nuclear installation, radiation monitoring systems are also applied to monitor the environmental radioactivity level far away from nuclear installation, such as radiation monitoring in border areas between countries. By the system, both the natural radioactivity and radiation release from other countries can be monitored. Thus, for radiation monitoring that carried out away from the safety monitoring center, a data transmission from monitoring point to the safety monitoring center is required. One of remote radiation monitoring system samples is the real-time Radiological Data Monitoring System (RDMS).

As a real-time system, measured data onto RDMS can be monitored far away from detector location. It is very useful and will be increased efficiency of the system. Besides to increase an efficiency of the system, the existence of data transmission network of RDMS also causes cybersecurity vulnerabilities. The main vulnerabilities are related to confidentiality, integrity, and availability of data or information. Thus, the RDMS application should be followed by cybersecurity measures.

This paper focus to discuss research purposed for implementing securing data transmission for radiation monitoring system in a nuclear installation. It's started by Section 1 that introduced to radiation monitoring system with related cybersecurity vulnerabilities, especially in data transmission. Section 2 illustrates the architecture of RDMS. It is followed by Section 3 that explores more detail the main vulnerabilities, including confidentiality, integrity, and availability of data or information related to the safety of the nuclear installation. Purposed research for implementing secure data transmission in RDMS that adopted or developed from some previous relevant research is presented in Section 4. Section 5 will conclude all of the paper.

2. ARCHITECTURE OF RDMS
A real-time Radiological Data Monitoring System (RDMS) is unity system for monitoring of radiation exposure or radioactive release level from nuclear installation. It consists of radiation sensor, signal processing unit, a micro central

processing unit, local memory, and transmission output. All of the units are supported by high voltage powers supply in their operations.

Radiation parameter, such as radiation exposure or radioactive contamination level, is received by a sensor and converted to current or voltage unit. This electrical parameter will be processed to amplify, convert, condition, etc., in the signal processing unit. The suitable signal can be computerized in a micro central processing unit to store in the local memory unit or transfer to the server computer in safety monitoring center through the suitable transmission network. Outside appearance and detail inside schematic diagram of RDMS are described in Figure 1.

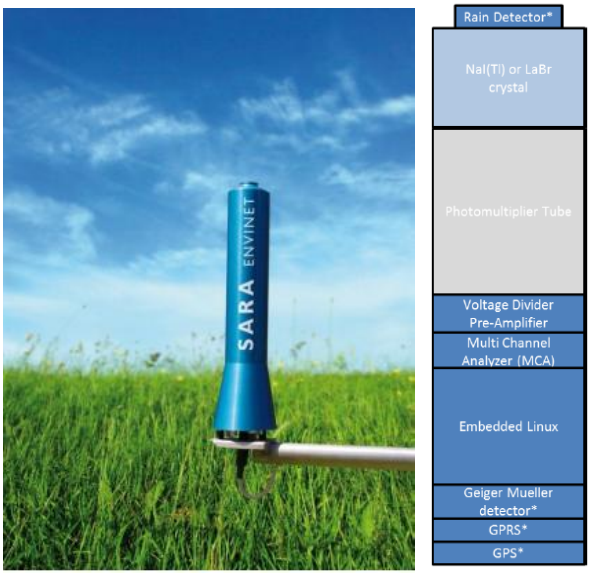

Fig. 1 Outside appearance, and detail inside schematic diagram of RDMS by Envinet (Envinet, 2017)

RDMS is equipped with two radiation detectors, a scintillation crystal, and Geiger Muller (GM) detector. Each detector has different function and range of radiation measurement. The scintillation crystal detector uses to measure very low radiation dose rate (slightly above natural radiation background). It can detect radiation dose rate range from 0.001 – 400 µSv/h. General scintillation crystal detector uses NaI(Tl) configuration. By NaI(Tl), detected particle or radiation generates light flicker. The light flicker then is multiplied or amplified by Photo Multiplier Tube (PMT) to produce suitable pulse or signal. Especially if radiation dose rate exceeding 400 µSv/h, the system will automatically perform the measurement with GM detector. It can detect radiation dose rate up to 100 µSv/h. It may be implemented in incident or accident condition.

For long distance detection system, output signal is transmitted through some remote data communication transmission, such as Local Area Network (LAN), Asymmetric Digital Subscriber Line (ADSL), General Packet Radio Services (GPRS), Universal Mobile Telecommunication System (UMTS), Long Term Evolution (LTE), radio, or satellite to central server at safety monitoring center. Figure 2 illustrates RDMS network structure designed by Envinet (Envinet, 2017).

In the central server at safety monitoring center, radiation data from tens, hundreds, even thousands of kilometers away from RDMS station is compiled and processed as suitable information. The information is stored in central memory or distributed to relevant stakeholders. The monitoring information, in such level, also can be shared as public information via the internet or other communication media.

Fig. 2 RDMS network structure designed by Envinet (Envinet, 2017)

RDMS can be implemented as area, ring, nationwide, or mobile monitoring system (Envinet, 2017). As an area monitoring system, the RDMS is used to monitor radiation in such area inside building or installation. If the system is implemented to monitor ring outside of area consists some installation, it's said ring monitoring system. In a nationwide monitoring system, RDMS installs in the country border to monitor radiation level, both from the own activities and other countries. Besides above conditions, RDMS also can be implemented to monitor radiation level in the activities of radioactive material transportation or in accident area as a mobile monitoring system. The description of monitoring model is presented in Figure 3.

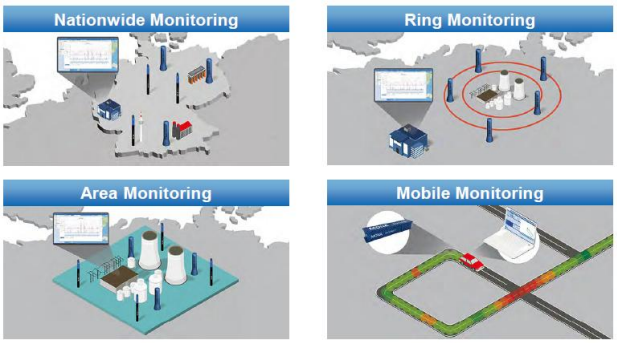

Fig. 3 RDMS implementation model (Envinet, 2017)

As a system to aggregate data from radiation sensor, the subsystem in RDMS can be identified some crucial point (in secure data communication context), including a process in measuring data from sensor, signal processing, local microprocessor, local memory, transmitter unit, transmission network, central server, until to the end user. Validity and accuracy of data are very important to gain valid and accurate information and to justify safety installation status or condition. Some potential vulnerability in all steps, such as data confidentiality, integrity, and availability should be managed. This purposed research is limited on how to design secure data transmission process from monitoring site to central server in safety monitoring center office.

3. DATA TRANSMISSION VULNERABILITIES IN RDMS

Nuclear installation is crucial and strategic facilities. Implementation of a digital system for industrial control systems in the installation, an especially data transmission process in the RDMS as described in the previous section, needs specific concern scheme in the context of cybersecurity vulnerability. The system has potential cybersecurity vulnerabilities, related to data or information confidentiality, integrity, and availability.

Based on Figure 2, it can be identified that RDMS connected to transmission or connection network through remote data communication transmission, such as Local Area Network (LAN), Asymmetric Digital Subscriber Line (ADSL), General Packet Radio Services (GPRS), Universal Mobile Telecommunication System (UMTS), Long Term Evolution (LTE), radio, satellite, internet, etc. RDMS can be connected to the unlimited network with the borderless connection. The network may be the secure or insecure system. In an insecure network, the cybersecurity vulnerabilities can be used by the adversary to access and exploit important or restricted data.
As a common industrial control system, in RDMS, the confidentiality, integrity, and availability of data or information are very impacted for the reliability of related industrial control systems. It is very important to determine the safety and security of overall nuclear installation. The cyber attack on RDMS can disturb radiation monitoring process and impact to the safety and security of the other system operation. More detail description of each impact is presented below.

Confidentiality of data or information is the property that data or information is not made available or disclosed to unauthorized individuals, entities, or processes (IAEA, 2011). In data transmission process as part of radiation monitoring system, a data confidentiality attacks can be launched by the adversary to find out information about the safety status of a nuclear installation in detail. Especially in incident or accident situation, such sensitive information may be misused or disseminated unwisely for conducting terror to provoke public fears. The anxious public will become more fearful. In this situation, sensitive and strategic information should be handled, managed, and delivered by competent authorities carefully and wisely.

Based on the targeted object, there are three types of cyber exploitation. They are server side exploitation, client-side exploitation, and man-in-the-middle (MITM) exploitation (NISA, 2017). Especially to exploit data confidentiality in data transmission process, the adversary can use all of the exploitation types above. The adversary can penetrate, enter, and exploit monitored data in RDMS, to conduct client-side exploitation. They can penetrate, enter, and exploit monitored data at the center server in safety monitoring center office as server-side exploitation attack. And the last, they also can act as a man-in-the-middle to exploit the data when it transferred through a connection network. By the exploitation, the adversary only wants to know and collect the data to be used as their objective. To conduct data confidentiality attack, the adversary should penetrate and connect to data transmission connection or network.
Integrity is the property of protecting the accuracy and completeness of data or information (IAEA, 2011). Inaccurate, fake, or modified data occurs when data transmission is exploited by the adversary with data integrity attacks. The information presented is not able to describe an actual situation, condition, or safety status of the nuclear installation. Normal discharge of radioactive material from the installation in safe and well operation can be indicated exceed the specified safety limit by an attacked data. Its situation can trigger public anxiety and fear that should be prevented. In contrast, radioactive material release that exceeds specified safety limit is not informed to relevant authorities. It causes early warning system does not work properly. The serious impact happens when incident or accident countermeasures cannot be conducted immediately. This situation is very dangerous for radiation safety to internal workers, members of the public, and the environment around the installation.
As well as data confidentiality attacks, data integrity can be exploited by all of the exploitation types. In contrast to data confidentiality attacks that attacker only want to know the data, in data integrity exploitation the adversary also modify, change, or falsify the data. By these attacks, the original or actual data is changed by falsifying data. The data destruction can trigger false information that will spread to false or un-accurate justification, decision, conclusion, or other assessment and action.

Availability is the property of being accessible and usable upon demand by an authorized entity (IAEA, 2011). In data integrity attacks situation, an accurate data couldn't be accessed by relevant authorities but radiation monitoring system or transmission networking still accessible. In cases of data availability attacks, the real radiation monitoring data, system, or network completely un-accessible. Thus, the relevant authorities don't know a real condition and safety status in monitored installation.

There are two ways to attack data availability in data transmission process. Physically, the adversary disconnects data transmission line or network and/or damage component or subsystem in the RDMS. By the attack, measured data cannot be generated or transmitted. As cyberattack action, the adversary can overwhelm the RDMS with falsify control command. In this condition, the RDMS cannot conduct radiation measurement perfectly. Thus measured data becomes unavailable. In another side, the adversary also can overwhelm the central server with falsifying monitored data or another request. In this situation, the central server cannot send a control command to the RDMS (downlink data cannot be done). In another scheme, the adversary can destruct or disturb connection reliability. Thus the RDMS and central server cannot connect each other, and data cannot be transferred. The above cyberattacks can be classified as Distributed Denial of Service attack (DDoS).

By reasoning as described above, there are some challenges to develop and implement securing data transmission for radiation monitoring system in nuclear installation related to confidentiality, integrity, and availability aspects of our purposed research below. To prevent all of the three cyber vulnerabilities as discussed in this section, it can be implemented authentication process for a new sensor, also encryption for data uplink and downlink process.

4. PURPOSED SECURINGG DATA TRANSMISSION IN RDMS

To applicate secure data transmission for supporting radiation monitoring system in a nuclear installation, this research proposes securing mechanism to the system by implementing security data communication protocol to authenticate for new RDMS, encryption both for uplink and downlink data process. Two different approaches will be implemented based on

implementation model of RDMS as single RDMS, or some RDMS that used in specified monitoring area together. For single RDMS, the system can directly communicate with the main server in monitoring central office. Especially for some RDMS that used in specified monitoring area together, one of the RDMS will be functioned as a local central gateway to communicate with the main server. Before transferring data to the main server, the other RDMS should send their monitored data to the RDMS gateway.

Some previous researchers in smart grid system will become basics or approaches to develop and applicate the security data communication protocol for RDMS system. For supporting algorithm protocol, it should be implemented suitable cryptography algorithm, both for encryption and decryption processing.

4.1 New Sensor Authentication

Each new RDMS should be authenticated previously before joint the system. Only monitoring data from authenticated RDMS can be received by the central server in monitoring central office. The Internet Protocol address of each new RDMS must be set up before it can send their monitoring data. This procedure is implemented to prevent spurious data from un-authenticated RDMS or unfamiliar system. By the mechanism, it can be made sure that monitoring data is valid to be processed and managed.

Some previous research on authentication mechanism for new equipment before joint secure data communication transmission system or network can be made as a basis for developing new RDMS authentication process. Authentication new smart metering in smart grid implementation has been researched in 2013 (Yan et al., 2013). The similar process to authenticate new sensor in transmission line as part of smart grid also has been conducted in 2014 (Fan et al., 2014) and in 2016 (Zhang et al., 2016). The authentication process for the new sensor in a transmission line that has been researched as mention above illustrates in Figure 4.

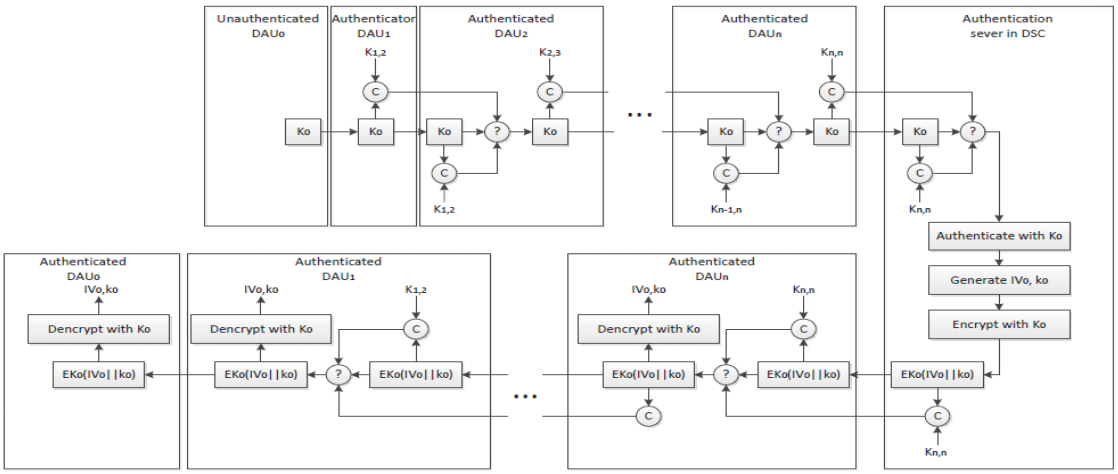

Fig. 4 Authentication process algorithm for new sensor in smart grid system (Fan et al., 2014)

In a smart grid system, each sensor node (Data Aggregation Unit, DAU) connects each other by the wireless serial connection. In communication with Data Switching Center (DSC), the sensor nodes connected through dual-link local gateway DAUs (DGD) by optical fiber composite overhead ground wire (OPGW).

The protocol of authentication process for new sensor as illustrated above works as indirectly communication between each DAU and DSC. In each node line, one of the DAU is functioning as a local gateway (DGD). The mechanism can be adapted and implemented in a situation when some RDMS are used in specified monitoring area together. The adaptation protocol of authentication process for the new sensor in smart grid system into RDMS system is described in Figure 5.

As describes in Figure 5, in this purposed research, one and others RDMS are connected as star connection with $RDMS_n$ as the local gateway. It is different from DAU connection in a smart grid system that implements serial connection. Thus each RDMS connects to $RDMS_n$ as the local gateway, and then just connects to the central server.

In the authentication process, new RDMS ($RDMS_0$) will request authentication to the central server via a local gateway ($RDMS_n$) by send authentication key (K_0). $RDMS_n$ will continue authentication request to the central server. By the central server, the request will be verified to make sure that $RDMS_0$ valid and can join to the system. If the central server declares or justifies that $RDMS_0$ is valid, it will generate initialization vector (IV_0) and identity key (k_0) for $RDMS_0$. The two keys will be sent to $RDMS_0$ through the local gateway ($RDMS_n$) after they are encrypted with K_0.

In a local gateway, the previous encrypted IV_0 and k_0 will be decrypted with K_0. By this mechanism, the local gateway knows all IV and k keys as an identification of all RDMS that connect to the central server. Finally, the authentication process will be finished by decryption of IV_0 and k_0 with K_0 in $RDMS_0$. After got IV_0 and k_0 as their identification keys, $RDMS_0$ has accepted to join the system. It can transfer monitoring data to the central server and also receive control or command data from the central server.

The authentication protocol mechanism as described above is suitable for area or ring monitoring model as illustrated in Figure 3, where some RDMS operated together in the specified area. An implementation of the local gateway will increase system efficiency and improve security capability of the system.

In another case, where only one RDMS operated in the specified location and far away from other RDMS (standalone RDMS), such as in-state border point, each RDMS should be connected directly to the central server. By this connection model, it is needed different authentication process for new RDMS before joining the system as illustrates in Figure 6. It is simpler compared to the previous system.

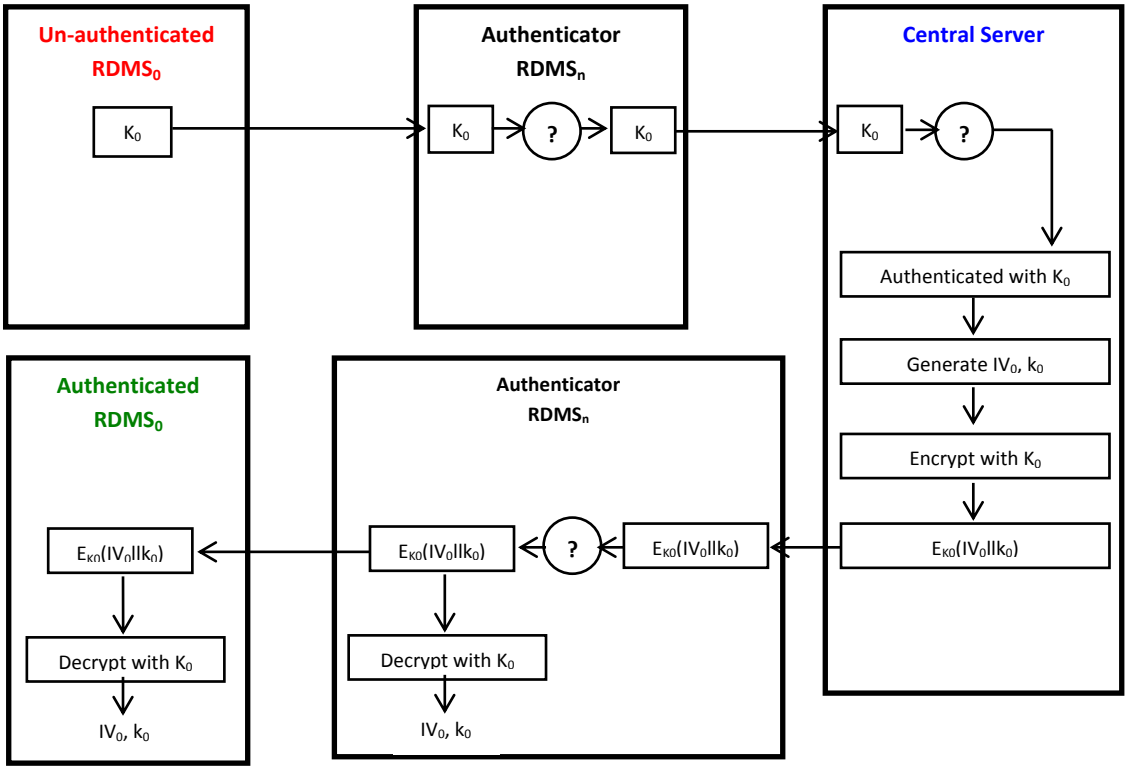

Fig. 5 Purposed authentication process algorithm for new RDMS un-directly to server (through local RDMS's gateway)

The authentication process for new $RDMS_0$ is started by sending of the connection request to the central server. It initiates by sending an authentication key (K_0) to the central server computer. When received initiate authentication key (K_0), the central server computer will verify to make sure that $RDMS_0$ valid and can join to the system. If the central server declares or justifies that $RDMS_0$ is valid, it will generate initialization vector (IV_0) and identity key (k_0) for $RDMS_0$. The identity key (k_0) and initialization vector (IV_0) are then encrypted by the central server computer and sent to $RDMS_0$. Thus the $RDMS_0$ has been identified by the central server computer with the application of adequate data security. Of course, this mechanism is simpler compared to authentication process un-directly through a local gateway.

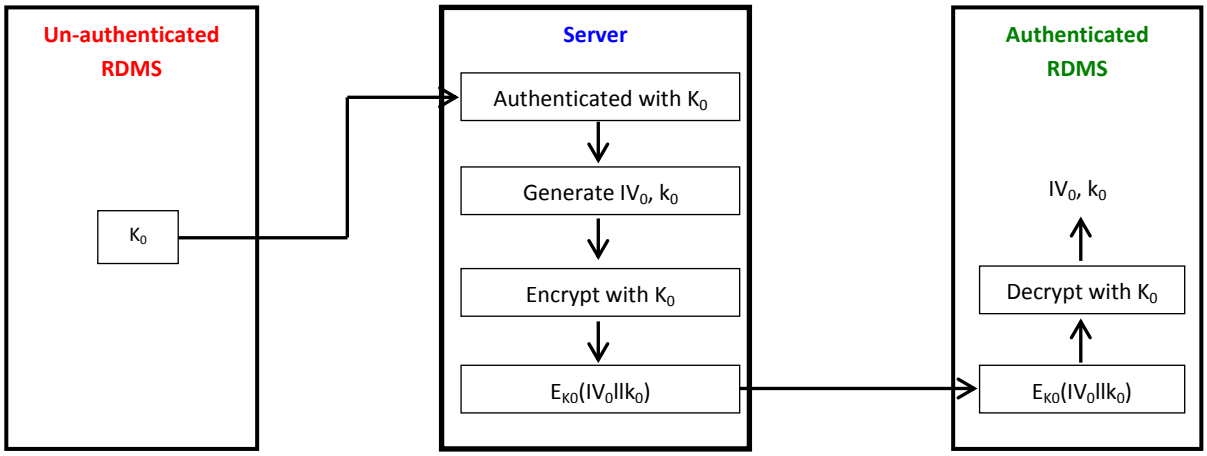

Fig. 6 Purposed authentication process algorithm for new RDMS directly to server

4.2 Encryption of Data Uplink

After such RDMS has been authenticated to the system, it can send monitoring data from detector to central server. This process defines as uplink data. To guarantee data security, the data should be encrypted before sending to the central server. Especially for smart grid system, encryption process for uplink data illustrates in Figure 7(Guo et al., 2014).

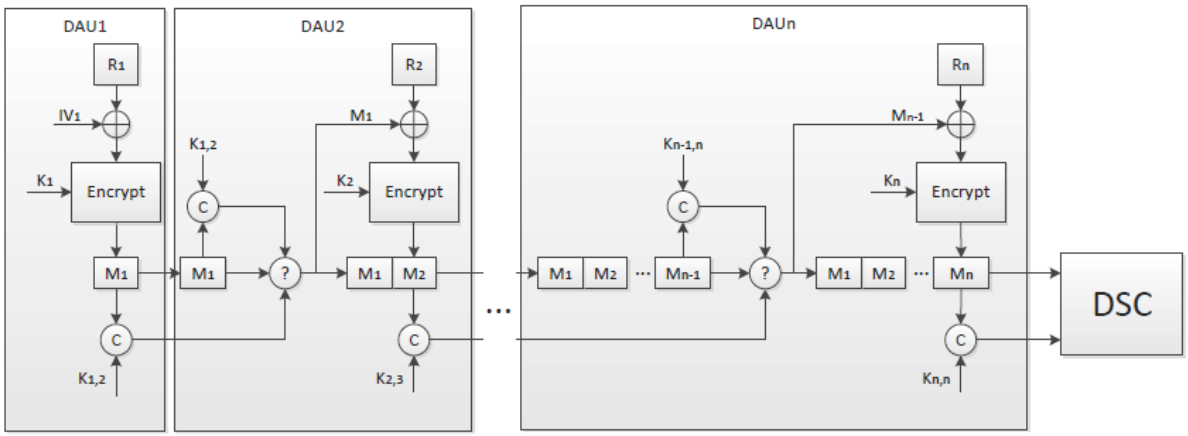

Fig. 7 Algorithm for uplink data encryption in smart grid application (Fan et al., 2014)

Based on an algorithm for uplink data encryption in smart grid application as described above, it can be adapted and modified the similar algorithm for RDMS application as illustrated in Figure 8 and Figure 9. The mechanism is differed based on RDMS monitoring model. The protocol developed, both for some RDMS that installed together in a specified area with the local gateway and standalone RDMS.

For the first case, it has been designed RDMS monitoring model with star configuration. In this configuration, communication from each RDMS to the central server should connect through a local gateway ($RDMS_n$). Radiation monitoring data from the detector in such RDMS (R_{1-n}) should be encrypted with initialization vector key (IV) and identity key (k). Both IV and k has been granted from the central server when authentication process conducted. They are very specific and unique for each RDMS.

After encryption process in each RDMS, encrypted message will be transferred to the central server via a local gateway ($RDMS_n$). In this mechanism, $RDMS_n$ operates as massages aggregator from the others. All messages will be sent to the central server together for some period time. In the central server, the received messages will be decrypted to get real measured data.

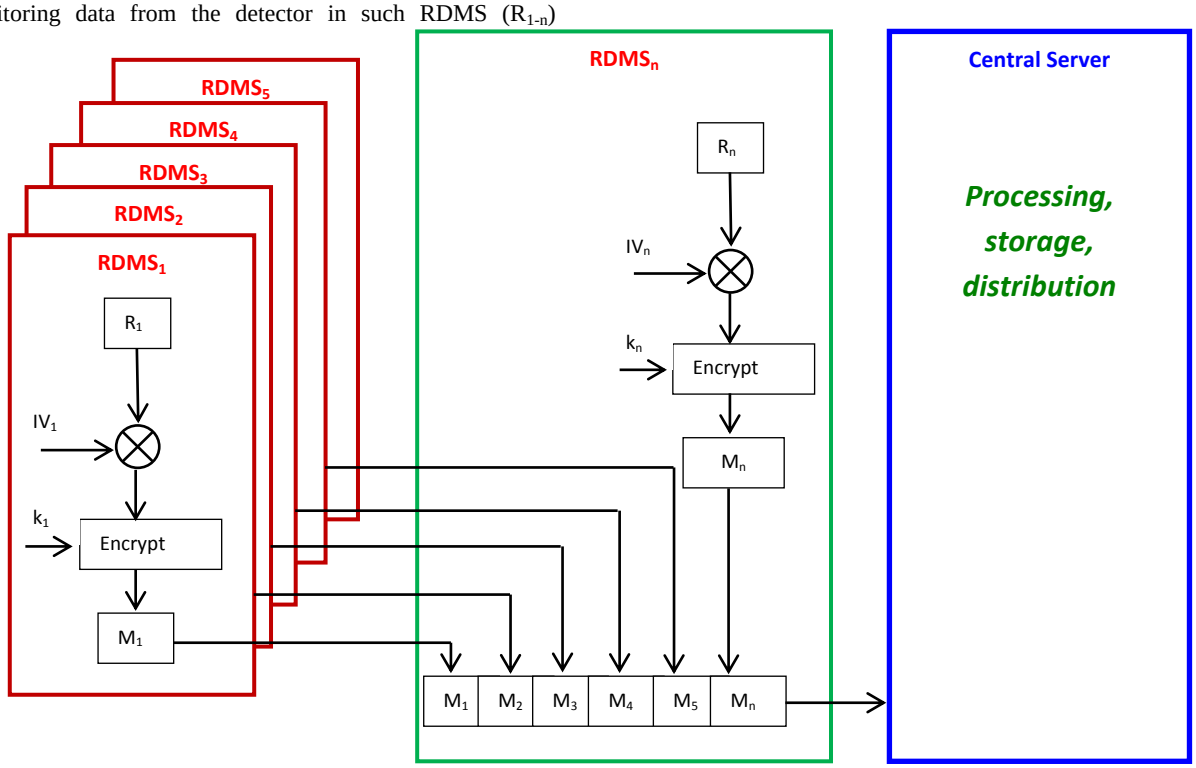

Fig. 8 Algorithm for un-directly uplink data encryption (through local gateway)

For standalone RDMS as described in Figure 9, the RDMS directly connect to the central server without a local gateway. Radiation monitoring data from the detector in the RDMS (R_1) are encrypted with initialization vector key (IV_1) and identity key (k_1). Both IV and k has been granted from the central server when authentication process conducted. They are very specific and unique for each RDMS. After encryption process, encrypted message will be transferred to the central server directly. In the central server, the received messages will be decrypted to get real measured data.

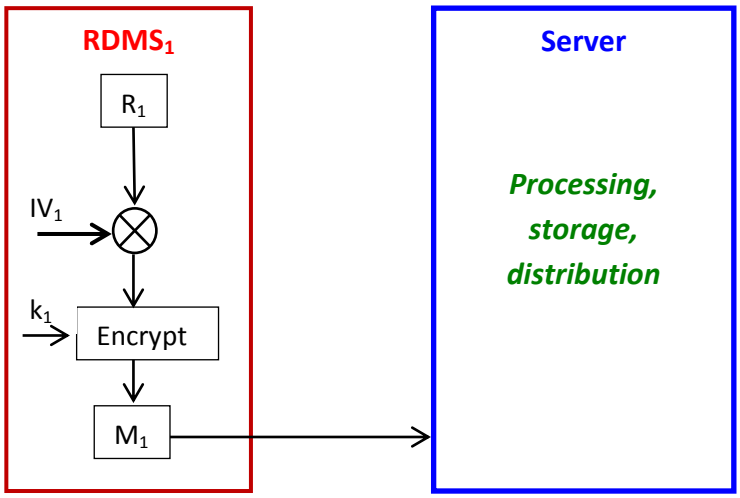

Fig. 9 Algorithm for directly uplink data encryption (without local gateway)

4.3 Encryption of Data Downlink

To support RDMS performance, bi-directional communication is needed. Downlink data means data transmission from the central server to all connected RDMS. Control messages, such as initial measurement setting or its changes, should be distributed to suitable RDMS. The control messages can be distributed as broadcast, unicast, or mono-cast. To ensure control messages security, it should be encrypted before sending to destination RDMS. The encryption process uses initialization vector key (IV) and identity key (k) for each suitable RDMS that conducted in the central server. Remember that each RDMS has unique IV and k generated by the central server when authentication process.

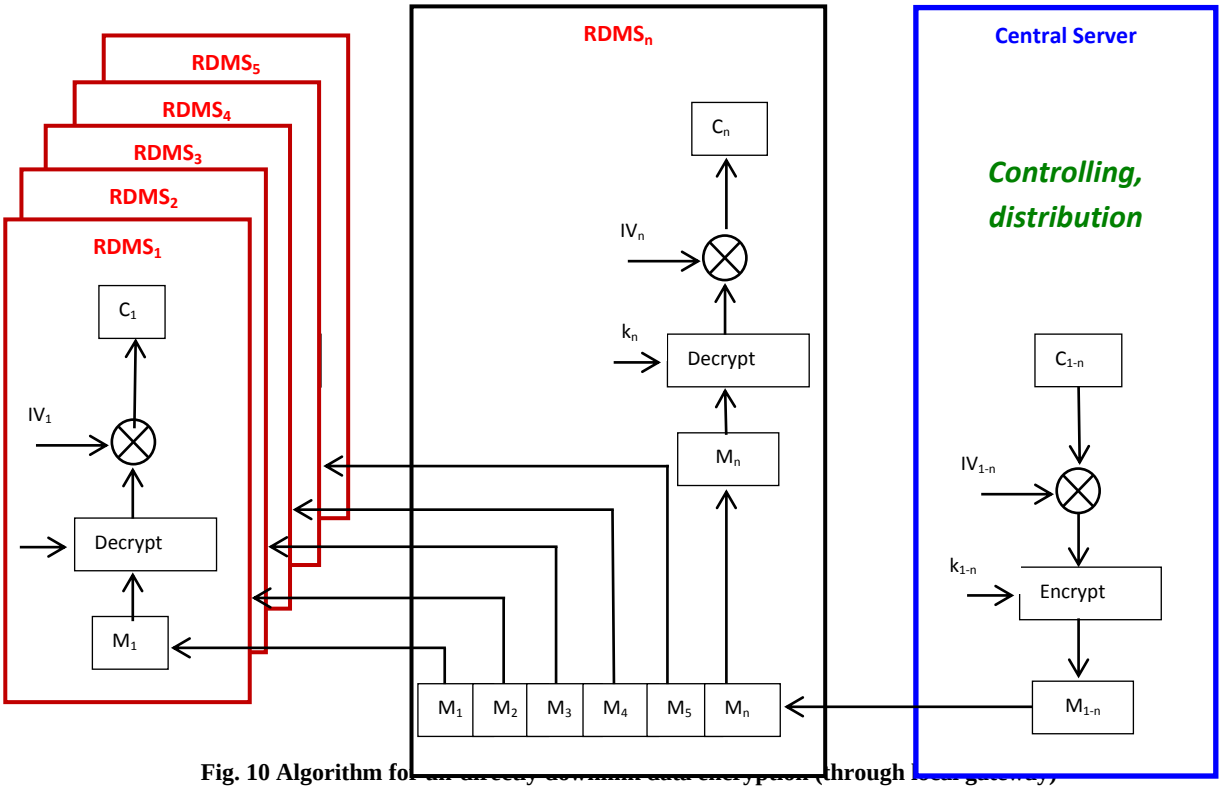

Fig. 10 Algorithm for [illegible] (through [illegible])

Figure 10 describes an algorithm for downlink data encryption through a local gateway ($RDMS_n$). In each destination RDMS, the control message should be decrypted with same initialization (IV) and identity key (k). By the process, each destination RDMS will get suitable control data as sent by the central server. The similar procedure will be executed for directly downlink data encryption for a system without a local gateway. The procedure describes in Figure 11.

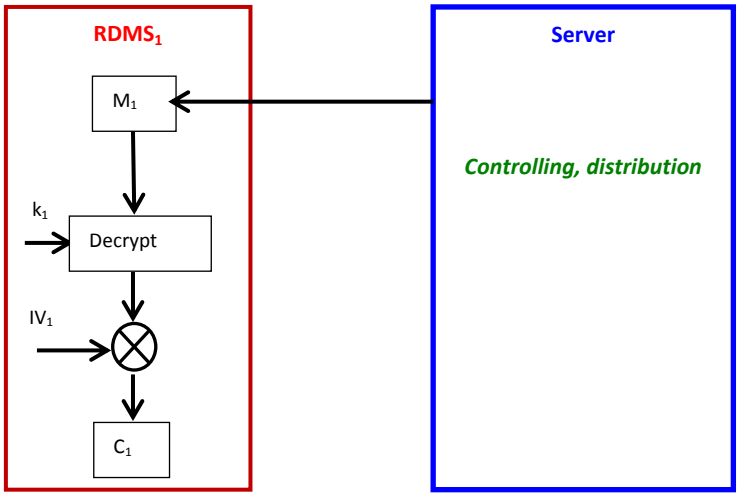

Fig. 11 Algorithm for directly downlink data encryption (without local gateway)

4.4 Purposed Cryptography Algorithm

Cryptography has long historical for securing in data transmission process. The main function of cryptography is data or information ciphering. Based on cipher keying utilization, it's differed symmetric and asymmetric cryptography. All purposed security algorithm as described in the previous subsection (authentication process, encryption data uplink, and encryption data downlink) implements symmetric cryptographic. Thus in the above protocol can be implemented some established and popular cryptography algorithm, such as Data Encryption System (DES), Advanced Encryption Standard (AES), Ron Rivest algorithm (RC), Blowfish, Carlisle Adams and Stafford Tavares algorithm (CAST), International Data Encryption Algorithm (IDEA), until Tiny Encryption Algorithm (TEA).

Dynamic research and development on symmetric cryptography techniques have entered into more modern and advanced cryptography today. Research for enhancing the security of AES against modern attacks by using variable key block cipher has been conducted (Sahmoud et al, 2013). Different with previous AES that implemented stream or block cipher techniques separately, their purposed research combines and uses both stream and block cipher techniques in one algorithm to add complexity and security. This mechanism is needed processing time about twice compare to previous AES.

(Alabaichi & Ibrahem, 2015) made research to enhance the security of advanced encryption standard algorithm based on key-dependent S-Box. In this research modification to previous AES conducted by adding one initial step each round (S-Box permutation). The terminology of dynamic AES related to dynamic utilization of keys for each round.

(Kaul et al., 2016) have been conducted research on next-generation encryption using security enhancement algorithms for end to end data Transmission in 3G / 4G Networks. The research has modified AES algorithm implemented on transport layer security (TLS). Purposed enhancement to previous AES, including utilization of chaotic system to achieve unlimited key dimension, and S-Box modification for generating dynamic cipher key utilization. For increasing system complexity, the AES was combined with round structure to generate non-linearity of the system. Evaluation of proposed system focused on encryption and decryption time, throughput speed and avalanche effect. The research result speed process 2 Mbps that will be compatible with LTE, more complex and attack resistance system, and of course the round number can be variated.

(Ganesh et al., 2011) have conducted research to improve AES-Elliptic Curve Cryptography (ECC) hybrid encryption scheme for secure communication in cooperative diversity based wireless sensor networks. The research was started by power supply limitation on wireless sensor network system, especially for supporting cryptography process. Increasing cryptography complexity should consider computation energy and time needed. Increasing digit number for a big cryptography key size can increase security complexity, but it is needed more energy supply. Ideally, it should be improved cryptography system with high complexity, but the size of the key is small. Implementation of ECC combines with AES has been improving security complexity without using the big key.

Besides research on cryptography system using a symmetric key, some related research on asymmetric cryptography also has been performed. In 2015, research on secured data communication system using RSA with Mersenne Primes and steganography has been done (Pund et al., 2015).

(Chaudhury et al., 2017) have conducted research on an asymmetric key-based cryptographic algorithm using four prime numbers (ACAFP) to secure message communication. The research has objective to modify Rivest Shamir and Adleman (RSA) algorithm. In previous RSA algorithm, both public and private keys were generated based on factorization of two big primes number. In modern RSA, for ensuring data security, it should be used primes number with size more than 1024 bits. Thus by the requirement, it is needed high supporting resources, such as energy consumption for encryption and transmission, long processing time, local memory, etc. Implementation of modified RSA (ACAFP) will decrease supporting resources. By the ACAFP, energy consumption for encryption and transmission are lower, processing time is faster, and little local memory is needed.

Different from the previous RSA, modified RSA uses four little primes number to generate public and private keys. Utilization of little primes number has a function to simplify computation encryption. Although it uses little primes number, it can generate a high level of data security. By mechanism, cryptography system will save resources, especially local memory and power transmission.

Regarding on advance research development of cryptography system as described above, it is very interesting to purpose modify algorithm that combined the newest algorithm with

other older algorithm. For symmetric cryptography system, it can be used combination AES with ECC. As established encryption standard by US National Institute of Standards and Technology, AES has a strong and a high level of security. The strong and high level of security generates from utilizing big size key (128, 192, and 256 bit). In another side, AES has achieved diffusion and confusion characteristics that approached ideal cryptography system.

Basically, almost all cryptography algorithm use big integer number for a security key. ECC give different approach by using small integer number, but security level is still high. For example, 160-bit security key generated by ECC has similar security level with 1024 bit security key in RSA (Stallings, 2006). ECC is very suitable to implement in a system with the limitation of resources, such system with a small microprocessor, small memory capabilities, small supporting power, etc. Algorithm combination between AES and ECC will increase security complexity of the system.

For asymmetric cryptography system, it can be proposed utilization ACAFP and ECC systems together. As explained by (Chaudhury et al., 2017) above, ACAFP simplifies size of the key without decreasing level of security. Implementation of modified RSA (ACAFP) will decrease supporting resources. By the ACAFP, energy consumption for encryption and transmission are lower, processing time is faster, and little local memory is needed. This protocol algorithm will be more powerful when combined with ECC. By combining ACAFP and ECC will increase security complexity of the system. To implement asymmetric cryptography protocol as ACAFP, all protocol or algorithm as discussed in the previous subsection should be modified to support it.

For choosing and implementing such suitable cryptography algorithm, it should be considered some important aspect, including configuration of system, capability of local microprocessor, and power supply capacity. It consideration also should be implemented in developing secure protocol algorithm for RDMS data transmission processing.

5. CONCLUSION

As digital and connecting to another system, application of Radiological Data Monitoring System (RDMS) to monitor radiation or radioactive release in nuclear installation generates some cyber vulnerability, especially in data transmission process. The vulnerabilities are related to data confidentiality, integrity, and availability. Based on smart grid system approach, it can be proposed some secure mechanism to protect data security for RDMS transmission process, including authentication of new RDMS, encryption of data uplink and downlink. The development of security protocol for securing data transmission in RDMS should consider the system configuration, capability of local microprocessor, and power supply capacity of RDMS. To increase security level, it can be proposed combination of some cryptography algorithm, such as AES and ECC for symmetric cryptography or ACAFP and ECC for asymmetric cryptography.

6. ACKNOWLEDGMENTS

Our thanks to Mr. Edi Winarko and Mr. Ahmad Ashari as the mentor and supervisor in the research.

7. REFERENCES

[1] Alabaichi, A., & Ibrahem, A. (2015). Enhance Security of Advanced Encryption Standard Algorithm Based on Key-dependent S-, 44–53.

[2] Chaudhury, P., Roy, M., Deb, S., & Roy, S. (2017). ACAFP : Asymmetric Key based Cryptographic Algorithm using Four Prime Numbers to Secure Message Communication. A Review of RSA Algorithm, 332–337.

[3] Envinet. (2017). *Environmental Radiation Detection*.

[4] Fan, S., Ye, F., Guo, J., Liang, Y., Xu, G., Zhang, X., … Engineering, E. (2014). A Security Protocol for Wireless Sensor Networks Designed for Monitoring Smart Grid Transmission Lines.

[5] Ganesh, A. R., P, N. M., Pl, S. S., Sundararajan, R., & Pargunarajan, K. (2011). An Improved AES-ECC Hybrid Encryption Scheme for Secure Communication in Cooperative Diversity based Wireless Sensor networks (pp. 1209–1214).

[6] Guo, Z., Ye, F., Guo, J., Liang, Y., Xu, G., Zhang, X., … Etwork, S. E. N. (2014). A Wireless Sensor Network for Monitoring Smart Grid Transmission Lines, 0–5.

[7] IAEA. Environmental and Source Monitoring for Purposes of Radiation Protection (2005).

[8] IAEA, I. A. E. A. (2011). IAEA Nuclear Security Series No. 17 Computer Security at Nuclear Facilities. *IAEA Nuclear Security Series*, (17).

[9] Kaul, V., Nemade, B., Bharadi, V., & Narayan, S. K. (2016). Next Generation Encryption using Security Enhancement Algorithms for End to End Data Transmission in 3G / 4G Networks. *Procedia - Procedia Computer Science*, *79*, 1051–1059. https://doi.org/10.1016/j.procs.2016.03.133

[10] NISA, U. (2017). Technical Introduction to Cyber Security at Nuclear and Radiological Facilities. Idaho: US NISA.

[11] Pund, S. (2015). Secured Data Communication System Using RSA with Mersenne Primes and Steganography, (2), 1306–1310.

[12] Sahmoud et al - 2013 - Enhancement the Security of AES Against Modern Attacks by Using Variable Key Block Cipher.pdf. (2013). *International Arab Journal of E-Technology*, *3*(January 2013), 17–26.

[13] Stallings, W. (2006). *Cryptography and Network Security (4th Edition)*. (M. J. Horton, Ed.) (4th ed.). Singapore: Pearson Prentice Hall.

[14] Yan, Y., Hu, R. Q., Das, S. K., Sharif, H., & Qian, Y. (2013). An Efficient Security Protocol for Advanced Metering Infrastructure in Smart Grid, (August), 64–71.

[15] Zhang, X., Ye, F., Fan, S., Guo, J., Xu, G., & Qian, Y. (2016). An adaptive security protocol for a wireless sensor-based monitoring network in smart grid transmission lines, (October 2015), 60–71. https://doi.org/10.1002/sec