Received: January 12, 2021. Revised: March 15, 2021.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

High Secure Initial Authentication Protocol based on EPNR Cryptosystem for Supporting Radiation Monitoring System

Nanang Triagung Edi Hermawan[1]
Edi Winarko[2]* **Ahmad Ashari**[2] **Yus Rusdian Akhmad**[1]

[1]*Indonesian Nuclear Energy Regulatory Agency, Indonesia*
[2]*Department of Computer Science and Electronics, Universitas Gadjah Mada, Yogyakarta, Indonesia*
* Corresponding author's Email: ewinarko@ugm.ac.id

Abstract: Radiation monitoring data is very important to support the safety of nuclear installation. The data should be ensured generated and supplied by an authenticated sensor. The new sensor should apply mutual authentication to server before joint the system. This research proposes a high secure authentication protocol based on Eight Prime Number of Modified RSA Algorithm (EPNR) method as certificateless mechanism to protect authenticity and confidentiality of sensor's identity. The main advantages of the protocol are designed for simpler direct point to point connection, using one-time random keys, and implementing five-barrier data protection mechanism. Its performances in context security, running time, and Quality of Services have been compared to other models. The proposed protocol is faster 29.9 times in random key generation, 7.27 times in encryption, and 11.1 times in decryption duration, compared to the others model based on RSA scheme. It has better performances in throughput and delay time. It also has enhanced resistance to statistical, replay, and MITM attack.

Keywords: Mutual initial authentication, EPNR algorithm, Five-barrier protection, Radiation monitoring system.

1. Introduction

Radiation monitoring system is part of safety related system in nuclear installation [1, 2]. The radiation monitoring data should be valid and correct to describe the installation condition related to radiation exposure or radionuclide release. The data describe an existing normal, incident, or accident condition of the installation. Data falsification, unauthorized modification, or unreal data can generate uncontrollable action by the operators or their related stakeholders [3]. The action can generate abnormal condition that can lead to very dangerous radiation incidents or accidents. It becomes very important to guaranty the integrity of radiation monitoring data.

Data and information integrity are very essential. Authentication procedures can be implemented to achieve the integrity. "Authentication is a process of verifying an identity claimed by or for a system entity" [4]. Basically, authentication can be divided into two categories, namely entity authentication and message authentication [4, 5]. A new monitoring device entity must be authenticated before joining the monitoring network [6]. The authentication mechanism is also mentioned as an initial authentication or registration procedure. In the mutual authentication, both the sender and the receiver of data must validate the authenticity of the corresponding party by acquirement of corroborative evidence [7]. The main goal of entity authentication is "to establish whether the claimant of a certain identity is in fact who it claims to be" [8].

Radiation Data Monitoring System (RDMS) is one of implemented radiation monitoring systems in nuclear installation. The RDMS has limited resources in their operation, especially in computational ability, memory, and battery capacity. This condition will influence a suitable implemented initial authentication method in the system [9]. An initial authentication should be conducted on an additional

equipment. A single board computer can be embedded to RDMS as additional machine for authenticating. Some suitable lightweight cryptography techniques should be implemented to ensure the device authentication in this system.

There are two model authentications based on cryptography techniques, namely certificate and certificateless authentication. In certificate authentication, the process needs some external parties, such as a minimum party likes registration authority, credential service provider, trusted-third party as certificate authority, and/or ticket-granting server [4]. A complex system, likes e-banking, e-transaction, and e-shopping, implement the method. In the context of simple system with limitation resources, certificate authentication is high cost and un-efficient [10]. A certificateless authentication method is more suitable for the system. It can be conducted by an asymmetric or public key cryptosystem. This authentication method is appropriate to the system which authenticates small number of devices and only between a server and the end-device [11].

RSA algorithm is the most popular public key cryptosystem that has been developed by Rivest-Shamir-Adleman in 1978 [4]. The method uses two different keys, called public and private keys. The receiver generates both of the keys. The sender uses the public key for encrypting plain text into ciphertext. This public key can be published through insecure line transmission. On the other side, the private key is used by the receiver for decrypting ciphertext into plain text. The private key should be kept secret and unpublished to anyone. Specific for authentication purposes, the sender generates the RSA key pair and distributes the public key to the receiver. The sender uses the private key for encrypting plain text into ciphertext. After receiving the ciphertext, the receiver uses the public key to decrypt the ciphertext into plain text.

As a public key cryptosystem, RSA needs the time-consuming, especially in random key generation and decryption processing to execute modular exponential operations. Related to system with capacity limitation, an authentication schemes based on public key cryptosystem are unsuitable [7]. In the context of RSA as authentication algorithm, it is needed modification of traditional RSA for solving the unsuitable. A modified RSA based on combination of multi-prime (more than two prime numbers) and the Chinese Remainder Theorem (CRT) method can be implemented to achieve the goals.

In the literature, there is no research on entity authentication of radiation monitoring system to protect confidentiality of device entity and monitoring data. In this article, we proposed High Secure Initial Authentication Protocol (HSIAP) based on an eight prime numbers of modified RSA algorithm (EPNR) method while still being double by the standard RSA. The strengths of our proposed method compared to previous protocols are:

a. dedicated to simple direct point-to-point network connection,
b. using different key in each execution
c. implementing multi-barrier security protections by double asymmetric cryptosystem, hash function, some blinding techniques, and timestamp mechanism.

We evaluate the performance of the proposed protocol through simulation experiments and security analysis. Experimental results show that the HSIAP protocol can provide efficient and secure communications with acceptable throughput, end-to-end delay, and packet loss.

The remainder of this paper is organized as follows. Section 2 discusses an existing RDMS communication architecture. Section 3 describes previous related researches. In section 4, we describe our proposed HSIAP based on an EPNR algorithm scheme. Section 5 presents and discusses the security, computational, and QoS performances of the HSIAP method. Section 6 contains conclusions and plans for future research direction.

2. Existing RDMS communication architecture

RDMS refers to systems that collect, measure, and analyse radiation exposure or radionuclide release from nuclear installation. It consists of radiation sensors, local mini processor, power supply, and data transmission system [9]. At each RDMS, sensor collects radiation exposure and radionuclide release data and send them directly to an application server. The system implements direct point to point network connections. Each node communicates directly to application server through Virtual Private Network (VPN) line. There is no communication between RDMS because the locations are different and far from each other. Fig.1 depicts a generic communication network architecture for RDMS system, which is generalized from the literature [12]. The system security relies only with the use of VPN line. If the security of the line can be hacked, then the security of the data becomes compromised.

To guaranty the integrity of radiation monitoring data source, the main requirement for RDMS security that should be fulfilled is device authentication. The identity and legality of the RDMS with associated

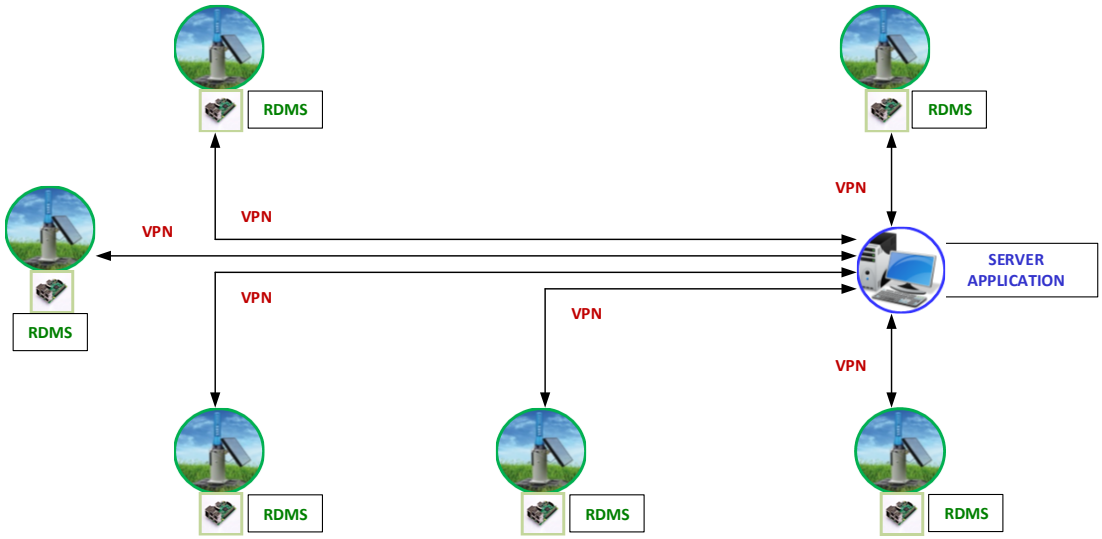

Figure. 1 An existing RDMS network architecture

information should be verified before joining the network. In the initial authentication process, some potential cyberattacks, such as statistical, factorization, replays, and man in the middle (MITM) attacks must be anticipated.

Regarding on resource constraints in an RDMS system, it needs lightweight but secure and efficient schemes tailored specifically for initial authentication process. The authentication protocol should implement modified cryptosystem that is fast and efficient (in terms of key generation, encryption, decryption, and total execution).

3. Related works

Some related researches to radiation monitoring have been conducted [13-16]. However, they were purely focused on local communication without considering outside communication and required security aspects, especially in mechanism of device authentication.

Although no similar, some previous related researches regarding the authentication protocol have been conducted in other areas. Such researches can be adopted, adapted, improved, and developed for radiation monitoring case. An initial entity authentication research in system with limited resources issues, such as in advanced metering infrastructure [17-22], smart grid transmission [23-33], wireless body area network [11,33-35], Vehicular ad hoc network or Internet of Vehicle [36-37], Internet of Things [10], and smart city data communication [38], have been interested.

In an advanced metering infrastructure, the new tools should be authenticated before joining the system. Authentication protocol employed mutual authentication between a remote server and a neighbouring smart meter as the authenticator to obtain proper cryptography keys for consequent secure data communications. The protocol was dedicated to network with multi-node and gateways. Storing and utilization of symmetric secret key in multi-hop chain wireless network generated security threat in secret keys storing and distribution [17].

Each new sensor in smart grid line should be authenticated to central control office through nearest node and gateway. The secure authentication protocol can be divided based on symmetric [23] and asymmetric algorithm [24]. The implementation of a secret key, also public key and private key for each node and each connection between two neighbouring nodes need complicated management to guaranty the key confidentiality. The scheme provides mutual authentication with protection against all known security attacks. An Elliptic Curve Cryptography (ECC) based lightweight authentication scheme also has been studied for smart grid system. However, the scheme could not provide mutual authentication and more time consuming compared to RSA scheme [26].

Proposed scheme in [33] implements hashing for wireless body area network (WBAN) authentication mechanism. The scheme has mutual authentication of two related node entities. It also used registered random number, and timestamp to improve security from replay attack. An efficient and certificateless conditional privacy-preserving authentication scheme for WBANs big data services is proposed in [34]. The proposed scheme supports batch authentication of multiple clients, which significantly reduces the computational overhead of the application provider. Moreover, the proposed scheme provides anonymity, unlink-ability, mutual authentication, traceability, session key

establishment, forward secrecy, and attack resistance. Another research related to universal forgery attacks on remote authentication schemes for WBAN also has been done [35].

Rathore et al. [38] proposed real-time secure communication for smart city in high speed big data environment. Their communication security protocol is included registration phase. Their protocol could enhance some security requirements, included authentication, confidentiality, integrity, and availability. Especially in using of RSA as asymmetric cryptosystem for more than 1024 bits of key size, the random key generation and decryption process can be improved by multi-prime numbers of modified RSA.

All above protocols are dedicated for complicated network with complex multi-nodes, multi-hopes, multi-gateway, etc. All of these schemes do not fit for the radiation monitoring application. It is needed different approach to develop simple and secure initial authentication protocol to be implemented in RDMS system. Regarding on this condition, we proposed HSIAP scheme for the system. The protocol was developed based on eight prime numbers of modified RSA method which implements multi-barrier protection mechanism.

4. Proposed method

The motivation of HSIAP development is to enhance secure and reliable certificateless authentication protocol that will be carried out on such embedded single board computer as part of RDMS. A double public cryptosystem is implemented in the protocol to achieve, both authenticity and confidentiality of the digital signature.

In key generation, standard RSA algorithm selects two prime numbers, p and q (which $p \neq q$). The modulus $n = p \times q$, and the Euler's totient number $\varphi(n) = (p - 1) \times (q - 1)$ are calculated. Based on selected integer e such that greatest common divisor $gcd\ (e, \varphi\ (n)) = 1$ (which $1 < e < \varphi\ (n)$), the private key $d = e^{-1} \bmod \varphi\ (n)$ is found. Then the pair of keys are a public key $PU = \{e, n\}$ and a private key $PR = \{d, n\}$. Encryption is calculated as $c = m^e \bmod n$, then decryption is calculated as $m = c^d \bmod n$, where c is the ciphertext, and m is the plaint message.

Fig. 2 shows the diagram of an EPNR algorithm as a basic of our proposed authentication protocol based on the dual variant of RSA. An application server generates a public key $PU_s(E, N)$ and private key $PR_s(D, N)$ based on two prime numbers (a, and b). The public key $PU_s(E, N)$ are sent to RDMS. The RDMS then generates another public key $PU_R(e, n)$ and private key $PR_R(d, n)$ based on eight prime numbers (p, q, r, s, t, u, v, and w). In the first encryption, the RDMS then uses $PR_R(d, n)$ to encrypt and authenticate the hash of RDMS's ID code ($Hash(ID_R)$) as M. The first encryption is calculated as $E_K(d, Hash(ID_R))$. The result then encrypted again with $PU_s(E, N)$ to produce a final ciphertext. The second encryption is performed as $E_{KD}(E, E_K(d, Hash(ID_R)))$. The final ciphertext (C) concatenated by $PU_R(e, n)$ are sent to application server.

After received the ciphertext, an application server uses $PR_s(D, N)$ in decryption process to get the encrypted $Hash(ID_R)$. In this decryption, the CRT method with two key exponents (Da and Db) is implemented. Finally, the application server uses $PU_R(e, n)$ in the second decryption steps and produce an original $Hash(ID_R)$.

Based on the above discussions, a comprehensive certificateless authentication protocol has developed. Fig. 3 describes a detail step by step of the protocol. The new RDMS should be registered before starting an above authentication procedure. The registration conducted by offline mechanism to guarantee identity information of new RDMS, such as name, location, type/model, and serial number. From this information, the server generates hash of RDMS's identity ($Hash(ID_R)$) and stores in database. The server always stands by to response each authentication request from new RDMS.

The registered RDMS can initiate an initial authentication by asking request to server. If the server is ready, the server send confirmation to the RDMS. In the same time, the server generates a pair of random keys based on RSA algorithm and send its public key to the RDMS. In another side, the RDMS generates other random keys based on EPNR algorithm. After receiving server's public key, the RDMS generates $Hash(ID_R)$ from RDMS's identity. The hash value is double encrypted and sent to server.

After receiving an encrypted hash value from the RDMS, the server decrypt it to get plain hash value. The plain hash value is compared to $Hash(ID_R)$ that stored in database. If they are identic, the server generates hash of server's identity $(Hash(ID_s))$, encrypt, and sends to the RDMS. After get $Hash(ID_s)$, the new RDMS has been authenticated by the system.

To enhance the confidentiality, each message is disguised by some agreed constants (K_1, …, K_6). Encryption techniques combined with hash, ASCII format, and disguise mechanism make multi-barrier protection from statistical, factorization, and MITM attack. Nonce and timestamp also are implemented in each communication to anticipate replay attack.

In order to evaluate the performance of our proposed authentication protocol based on EPNR

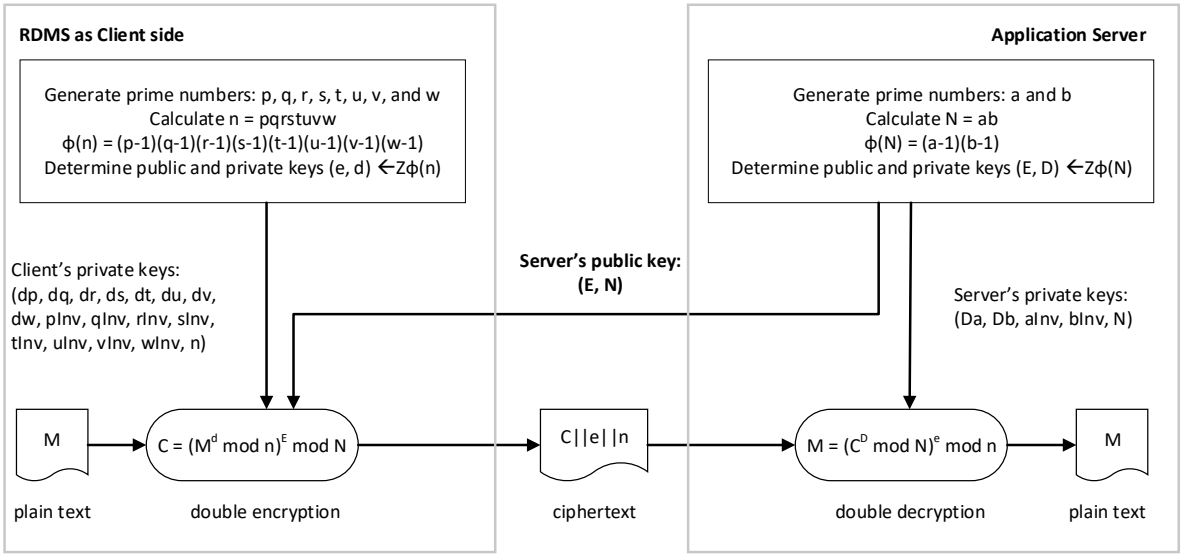

Figure. 2 An EPNR algorithm as fundamental of proposed protocol

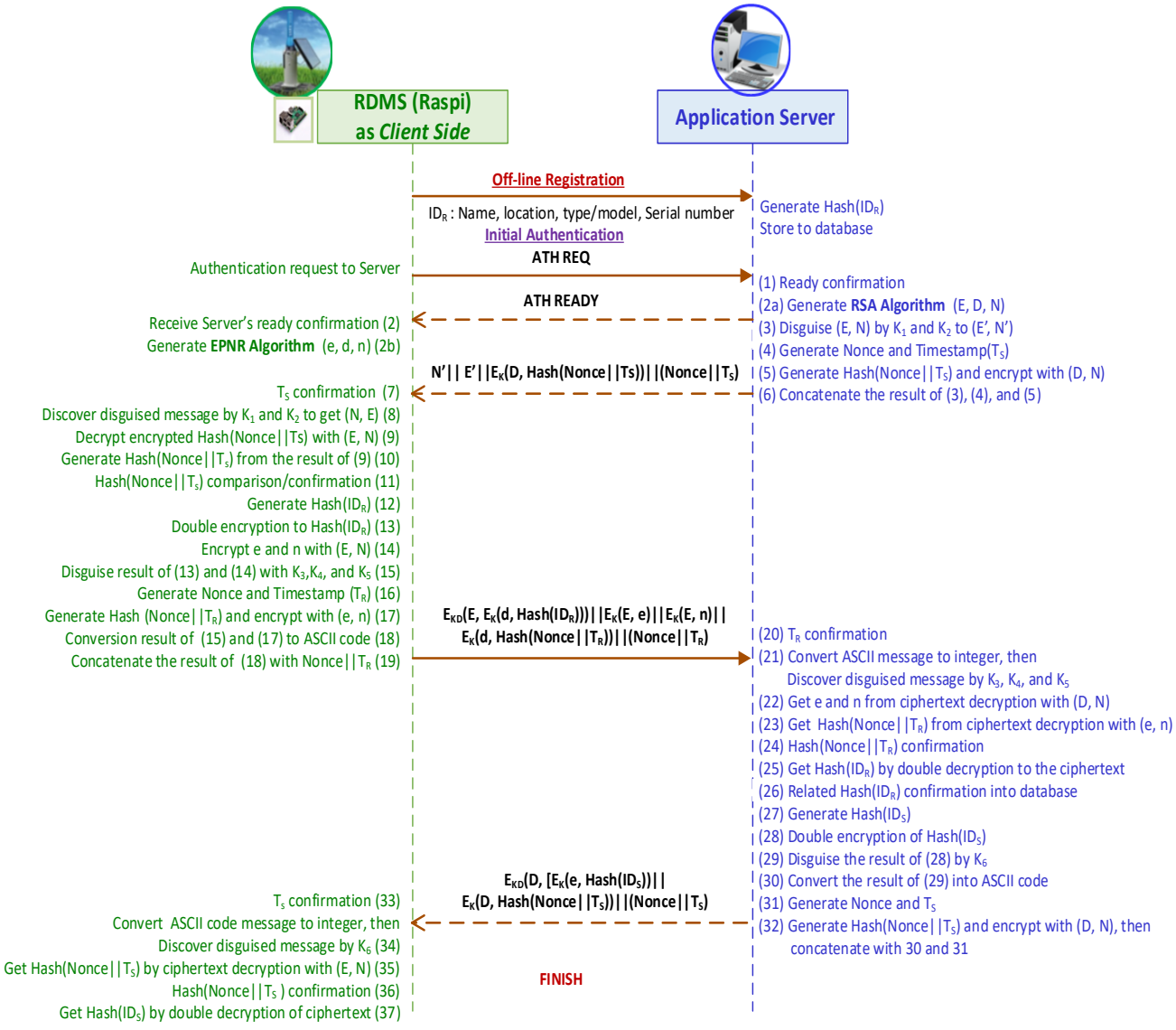

Figure. 3 HSIAP: an authentication scheme based on EPNR algorithm

cryptosystem, we have compared it to the same protocol schemes that was ran based on standard RSA algorithm and another modified RSA algorithm with four prime numbers (that is called ACAFP algorithm) [39]. We implement these protocol in Python 3.8 and run them in a Raspberry Pi 4 Model B and a Laptop that connected through LAN Ethernet cable. The Raspberry acted as a client side (RDMS side). In another side, a Laptop with Intel®Core ™ i3-4030U CPU@1,90 GHz processor, 8.00 GB RAM, x64-based 64-bit, and Windows 10 Pro Operating System acted as a server application side (server side).

5. Results and discussion

We perform theoretical system comparation based on relevant previous model and experiment execution to analyse performances of our proposed protocol. In experiment execution, we perform three sets of experiments. The first experiment is to compare theoretically the resistances of the protocols from statistical, replay, and MITM attack. The second experiment is to compare the running time of random key generation, encryption, and decryption steps. The third experiment is to compare the Quality of Services of the network connection between client and server side. In these experiments, we varied the size of key (in bits), that is, *800, 1024, 1600, 2048, 3200, 4096, 5000, 6000, 7000,* and *8192*. For more deeply analysis, we compared our proposed protocol based on three different mechanisms of RSA variant (standard RSA, ACAFP [39], and EPNR).

5.1 System comparison

The main concern of the initial authentication protocols for radiation monitoring system is to consider simpler direct point to point connection network. Based on limited research for securing authentication of device in this field, we compared our model to some previous relevant research in other fields. Table 1 shows the comparative study with above relevant existing works.

From Table 1, we know that our proposed model especially very different in network topology compared to others. The most advantage of our model

Table 1. Comparative study with existing relevant works

System environments	**AMI** [17]	**Smart Grid** [24]	**WBAN** [33]	**Smart City** [39]	**Proposed model**
Network:					
• Complexity	Complex	Very complex	Complex	Very complex	Point to point
• Gateway	Exist	Exist	Exist	No exist	No exist
• Line	Wireless	Wireless, optic	GPRS/edge	Wireless, internet	Internet (VPN)
Pre-auth.:					
• On/off-line	on-line	off-line	off-line	off-line	off-line
• Based on	Asymmetric key	installed key	registered num.	required inform.	ID hash value
Cryptosystems:					
• Algorithm	Symmetric	Hybrid	Hash	RSA/ECC	RSA and EPNR
• Used key	Static	Session keys	No key	Session key	One-time key
• Auth.	HMAC	Not exist	Hash digest	Blake2b	SHA-256
• Mechanism	Single	Single	Single hash	Double	Double
Auth.:					
• Directly	No	No	No	Yes	Yes
• Via gateway	Yes	Yes	Yes	No	No
Protection	1 layer	1 layer	1 layer	2 layers	5 (multi-barrier)
Handshakes	8	8	2	5	5
Auth. output	Asymmetric, Communication key	Public key, Communication key	Registered ID, random number	Stamped ID	Verified ID hash value
Attack anticipation:					
• Replay	No anticipated	Nonce/timestamp	Timestamp	Nonce/timestamp	Nonce/timestamp
• Statistical	Encryption	Encryption	Encryption	Encryption	Encryption
• MITM attack	Encryption	Encryption	Encryption	Encryption	Encryption +ASCII format

Note: *AMI (Advanced metering infrastructure); WBAN (Wireless body area network); auth.(authentication); ID (identity)*

Table 2. Complexity comparison of the various phases

Research	Total complexity	NME*
AMI [17]	$1T_{SKG}+2T_{SE}+2T_{SD}$	8
Smart grid [24]	$3T_{SKG}+2T_{SE}+2T_{SD}+1T_{AKG}+mT_{AE}+mT_{AD}+9T_{H}$	8
WBAN [33]	$1T_{NT}+4T_{H}$	2
Smart city [38]	$2T_{AKG}+9T_{AE}+9T_{AD}+3T_{NT}+6T_{H}$	5
Proposed model	$2T_{AKG}+8T_{AE}+8T_{AD}+3T_{NT}+4T_{H}$	5

*Note: NME (Number of message exchange); m (number of nodes)

was implementation of multi-barrier protection in each data communication. It barrier was constructed by hashing, the first and second encryption, disguise with such agreed constant, and ASCII format mechanism. It is very useful to protect RDMS's identity confidentiality from un-authorized party.

The system efficiency is very related to total computational cost in terms of time consumed. Theoretically it can be represented by the total authentication running time that is depended to each step process execution. Table 2 presents time consumed comparison of our proposed protocols and previous relevant study. It is included time consumed for asymmetric key generation (T_{AKG}), asymmetric encryption (T_{AE}), asymmetric decryption (T_{AD}), symmetric key generation (T_{SKG}), symmetric encryption (T_{SE}), symmetric decryption (T_{SD}), nonce and timestamp generation (T_{NT}), and hash generation (T_{H}). It comparison excluded data communication duration.

Table 2 shows that the WBAN protocol is the simplest, but also the most unsecure model. It only uses hashing mechanism on data protection. The most complicated model is smart grid. It works based on symmetric cryptosystem, but also generates and uses asymmetric algorithm for distributing symmetric keys. Its performances also are influenced by the number of connected nodes in the network system.

Our proposed protocol is identic with the smart city model in term of operating based on asymmetric algorithm and preventing integrity, replay, or MITM attack. However, our model has slight advantages related the number and efficiency on encryption-decryption and hashing execution. It is also dedicated for simple network and specially for radiation monitoring system with five barriers of data protection. The implementation of barriers needs a little extra time execution, but it can improve security significantly.

5.2 Security comparison

The security performances of the proposed method related to protocol resistance to statistical, replay, and MITM attack are discussed here.

5.2.1. Resistance to statistical attack

The resistance of the proposed authentication protocol to statistical attack is represented by bits randomization level. The bits randomization level of ciphertext is represented by Shannon Entropy value *H(x)* in Eq. (1). The ciphertext with higher *H(x)* value will be more difficult to decompose by an attacker. The value is calculated from [40] and [41]:

$$H(x) = -\sum_{i=1}^{n} p(x_i) log_2 p(x_i), \quad (1)$$

where $p(x_i)$ is a probability of such character appear in all sets of total characters that observed *(n)*. Table 3 describes the determination of Shannon Entropy values based on RSA variant schemes.

Based on Table 3, there are no significantly different Shannon Entropy values for different schemes. The values are high (close to 8, the maximum Shannon Entropy value). It is mean that all schemes generated ciphertext with high resistances from statistical attack. The entropy value is independent from type of cryptosystem, however heavily influenced by character code being used. Based on ASCII code used, our model theoretically always has a higher entropy than others, includes smart grid [24] and smart city [38].

Table 3. The Shannon Entropy value of ciphertext (in bits)

Size of keys (bits)	Scheme (based on)		
	RSA	ACAFP	EPNR
800	7,28	7,29	7,29
1024	7,45	7,45	7,46
1600	7,67	7,68	7,68
2048	7,74	7,76	7,75
3200	7,85	7,86	7,86
4096	7,88	7,89	7,88
5000	7,92	7,91	7,91
6000	7,93	7,93	7,93
7000	7,94	7,94	7,94
8192	7,95	7,95	7,95

5.2.2. Resistance to replay attack

"A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed" [38]. In authentication processing, an attacker might replay any request from the client towards to the application server, and vice versa.

There are two mechanism that implemented to anticipate the replay attack in our proposed protocol. They are off-line registration and nonce-timestamp mechanism. The mechanisms also are described in Fig.2. Firstly, the new RDMS, as client side, should send their identity information completely. The mechanism is conducted off-line as pre-registration step. Based on off-line registration, the server clarifies and generates specific identity and its related hash value. Only registered new client can continue to request for on-line authentication based on our protocol. By the mechanism, un-registered that might be an attacker could not be authenticated.

The second mechanism is nonce and timestamp implementation at each communication data. These nonce and timestamp are hashed and signed as $E_K(d, Hash(Nonce||T_R))$ and $E_K(D, Hash(Nonce||Ts))$ that is also described in Fig.2. The proposed authentication protocol has mechanism to checks the hash value of nonce and timestamp when receiving the data. In addition to ensuring the authenticity of the client and server, this step also checks the freshness of the message. Freshness time limitation was added to filter the dubious message. The mechanism can be guaranteed that no alteration can be conducted by an attacker. Thus, there is no replay attack can be performed to our model.

Our model implements hash and signature nonce/timestamp as a smart city model [38], however we also added freshness checking. The two previous anticipations were not conducted in other models [17, 24, 33].

5.2.3. Resistance to MITM attack

"Man in the middle attack is normally performed for getting access to the information that is sent from source to the destination while in-between the transmission" [38]. MITM attack simulation has been conducted to test the authentication protocol mechanism. The simulation used Ettercap tool. It is a sniffing tool available in the Kali Linux operating system [42]. It was combined by Wireshark to capture and analysis the packet.

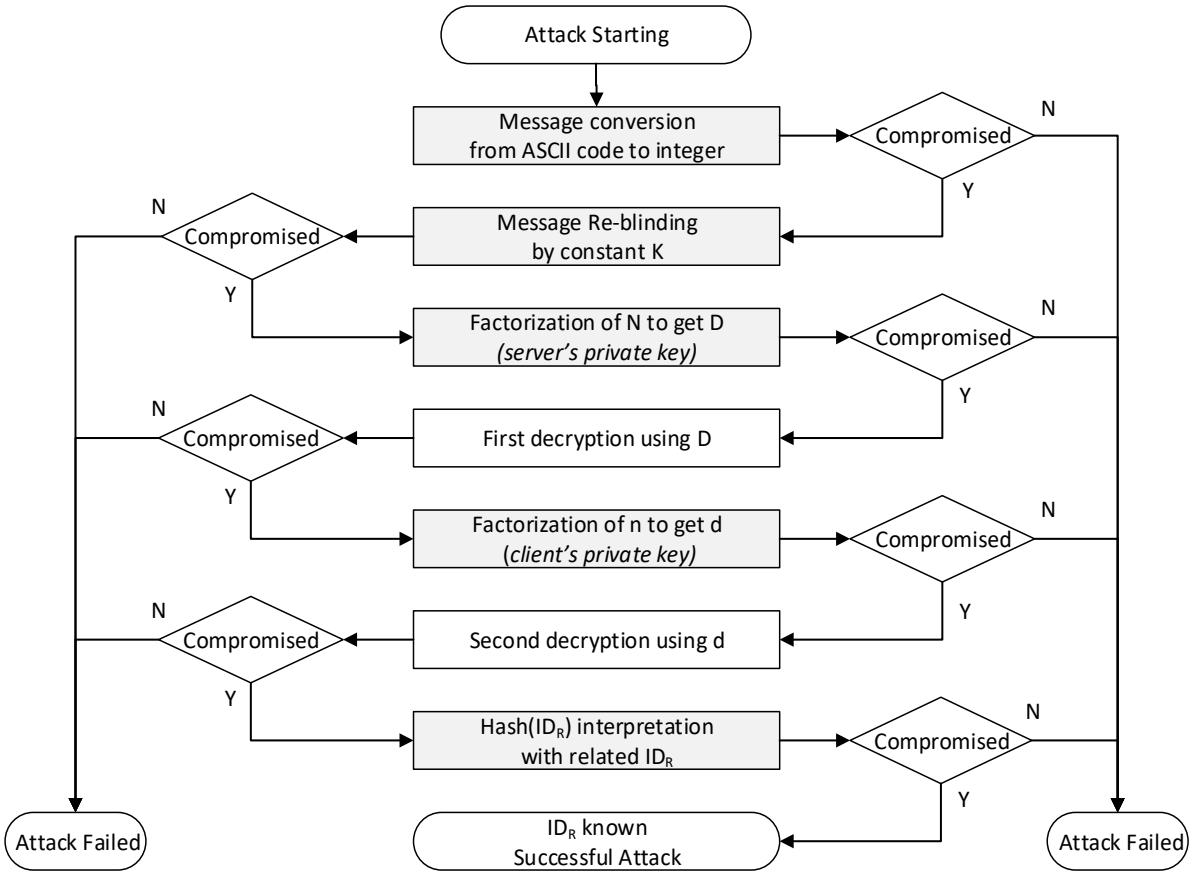

Figure 4 Multi-step penetration to compromise the five-barrier protection model

Although the attacker can carry out the MITM attack, they just got an encrypted data. The hashing to identity, a double strong encryption, blinding or undercover act to ciphertext, and conversion the ciphertext to ASCII code mechanism make multi-barrier protection to the plain text. It protection is a very strong implementation of defence in depth concept for our authentication protocol.

Especially the double encryption mechanism, it protects both confidentiality and authentication of our digital signature. By implementing five barriers protection, the attacker should conduct extra penetration to compromise our system. Fig. 4 depicts step by step hard effort to crack our model protection. By assumption the attacker doing the hard effort to crack the fifth and the fourth outer barriers, they should conduct factorization attack to the double encryption of RSA variant. As we know that the largest such semiprime yet factored was RSA-250, an 829-bit number with 250 decimal digits, in February 2020. The total factorization computation time was roughly 2700 core-years of computing using Intel Xeon Gold6130 at 2.1 GHz [43]. It factorization used General Number Field Sieve (GNFS) method. Based on computability resources, the above factorization attack only can be conducted by attacker with very high resources.

In the double encryption processing at client side, the first encryption was conducted using an EPNR algorithm that is modified RSA based on eight multi-prime numbers. In the context of algorithm's resistance to GNFS attack, implementation of eight multi-prime numbers will reduce its resistance to one eighth compared to standard RSA.

The standard RSA is still applied to the second encryption to overcome the previous vulnerability. Thus, if the resistance to factorization attack in dual standard RSA scheme is doubled, then our proposed EPNR method only increase by one eighth. By this mechanism, the random key generation and encryption in client's side (incidentally on single board computer environment) can be accelerated with still ensuring security from GNFS factorization attacks. Our experiment very recommends to use RSA cryptosystem with minimum key size 2048 bits. The strength of our protocol also was added by one-time utilization of random key pair mechanism. It means that our multiple-barrier is very strong to protect our digital signature confidentiality.

Beside conducting multi-barrier protection scheme, the authentication protocol also implements hashing mechanism. It makes sure that the data is not changed, modified, or destructed by any adversary. It might also be possible in the MITM attack that an adversary just changes all the information in the packet and add his information or messages in the packet then send to the destination presenting to be a legal source. However, we used powerful digital signature mechanism by using double public key cryptosystem to make sure that the data is coming from the authentic user.

Based on previous study, the smart city model [38] has only two barriers by double encryption mechanism to protect data from MITM attack. The other models [17,24,33] depend on single encryption or hashing to do that. It can be summarized that our proposed protocol has more advantages to anticipate MITM attack compared to others.

5.3 Running time comparison

The main processing in our proposed protocol is related to an EPNR operation. It is included random key generation, encryption, and decryption processing. Based on different algorithm compared to previous relevant studies, they cannot be compared directly. We compared the running time of the proposed protocol to two different schemes based on standard RSA as basic, and ACAFP [39]. The algorithm is generated both at client and server side, but our discussions are focused at client side. As we know, the server always uses standard RSA in our scenarios. The running time on random key generation, encryption, and decryption are described in Fig. 5, 6, and 7.

Generally, it can be seen in Fig. 5, 6, and 7, that for increasing the longer size of keys or system modulus (n), the time processing will also increase exponentially for all of the schemes. In the same size of keys, it can be compared more rigid, increasing speed up on the process based on the utilization of multi-prime numbers for the same key size.

Our proposed scheme based on EPNR algorithm is fastest in all three processes. As listing in Table 4, the EPNR's speed compared to others are: 29.29 compared to standard RSA and 3.15 compared to the ACAFP [39] in random key generation, 7.27 compared to standard RSA and 1.65 compared to the ACAFP in encryption, and 11.1 compared to standard RSA and 3.18 compared to the ACAFP in decryption.

The most important requirement in key generation of RSA cryptosystem is to use a big integer of a private key ($d \geq \frac{1}{3} n^{1/4}$) for avoiding Wiener attack [44] and brute force attack [4]. The proposed system always fulfils the requirements.

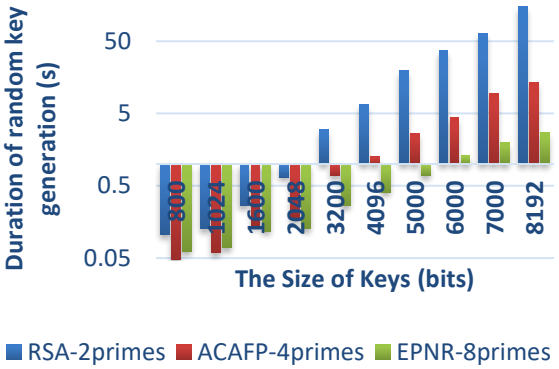

Figure. 5 The running time comparison of the random key generation (in logarithmic scale)

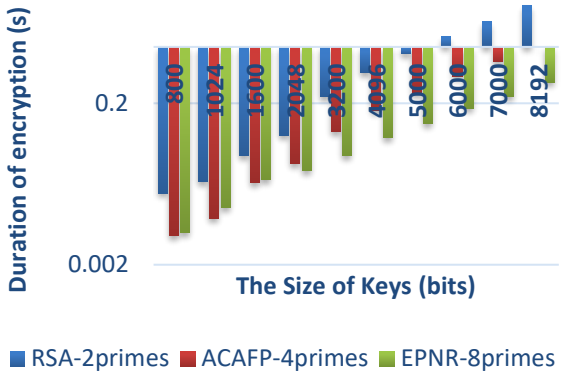

Figure. 6 The running time comparison of the encryption processing (in logarithmic scale)

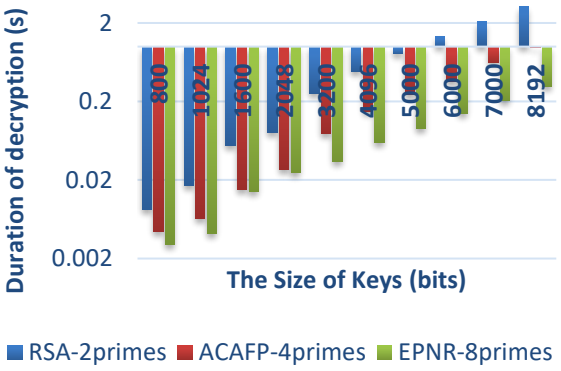

Figure. 7 The running time comparison of the double decryption (in logarithmic scale)

The main different of our proposed protocol compared to previous model is that both public and private key are used once times. In different execution, the different keys are used. It will be difficult for attacker to compromise the keys.

The mechanism to generate keys need extra time in each execution, but it does not require security and store of keys in the system as in the smart grid [24] and smart city models [38]. Compared to other models based on symmetric cryptosystem [17,33, 45], our proposed protocol does not need secure key distribution.

Especially in double encryption/decryption processing, the two processes are identic. Both public and private key components are used in the process. The specific different of the two mechanism is only in case of public and private key utilization and the sequence of steps to reversed. However, their time performance is also identic. Compared to other models based on symmetric cryptosystem [17,33, 45], our proposed protocol needs more extra time in encryption/decryption processing [46]. However, each client in our model is directly connected to the server when authenticating, so the process to be fast. This is very different from systems that have many nodes and are connected serially [17,45]. They need more processing based on the number of nodes.

Table 4. The fastest EPNR scheme processing compared to others

Processing	EPNR scheme compared to	
	Standard RSA	ACAFP
Key generation	29.29	3.15
Encryption	7.27	1.65
Decryption	11.10	3.18

5.4 End-to-end Quality of Services

Quality of Service (QoS) in the field of telecommunications can be defined as “a set of specific requirements provided by a network to users, which are necessary in order to achieve the required functionality of an application (service)” [47]. In another reference, quality is defined as “the totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs” [48]. In our proposed authentication protocol as a part of network communication protocol, QoS very influences entirely system performances.

In this subsection, three mains of QoS parameters, namely throughput, delay, and packet loss are discussed. The parameters support our proposed authentication protocol. Each QoS parameters was tested based on three different mechanisms (RSA, ACAFP, and EPNR). Our experiments use Wireshark, a packet analysis application, to capture the QoS parameters.

The first QoS parameter is throughput. Throughput is an effective rate at which packets go through the network. Greater throughput means the

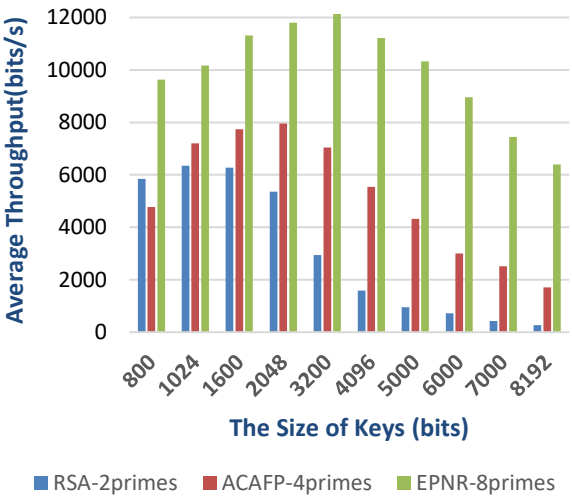

Figure. 8 Average throughput performances

network transmit data more effective. It means increasing of throughput will increase effectiveness of the network. Fig. 8 presents the average throughput comparison of the authentication process.

Regarding on throughput definition, end-to-end process on each side of the communicant greatly affects the effectiveness of using the connected network. In our experiments, the length of time processing on key generation, encryption, and decryption determines the throughput. As discussed at previous subsection, multi-prime numbers implementation in our authentication protocol very influencing each mentioned processing (in the context of time processing), and then also impacting to the throughput. Fig.8 shows that implementation of the protocol based on EPNR scheme has the biggest average throughput compared to RSA and ACAFP schemes by comparison factor 7.6 and 2.1. Especially for EPNR scheme, the graph indicates an optimum key size with maximum throughput in our system is 3,200 bits.

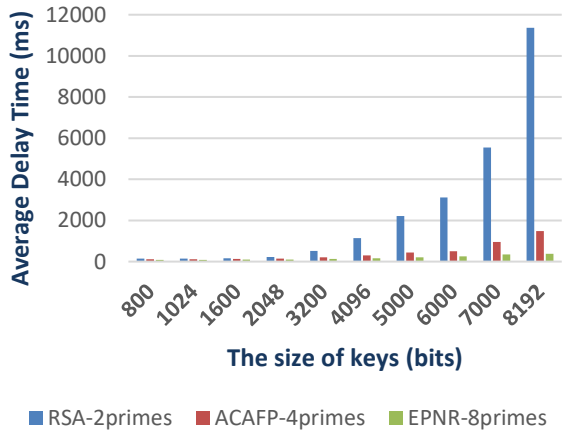

Figure. 9 Delay time performances

Table 5. Delay time performance of the proposed authentication protocol

Key size (bits)	Schemes (based on)		
	RSA	ACAFP	EPNR
800	137,497***	113,319***	83,792***
1024	137,733***	115,891***	86,736***
1600	167,674**	132,539***	95,331***
2048	223,245**	145,535***	104,064***
3200	518,394#	204,759**	125,076***
4096	1139,699#	306,766*	160,899**
5000	2208,066#	437,624*	202,262**
6000	3121,047#	503,724#	251,329**
7000	5542,539#	949,754#	340,732*
8192	11356,716#	1482,532#	382,744*

ITUT standard on delay time performance, ***Excellent (t_d < 150); **Good (150 ≤ t_d < 300); *Poor (300 ≤ t_d < 450); #Unacceptable (t_d > 450) [49]

The second QoS parameter is the delay time. The delay time is time taken by a packet to travel through the network from one end to another. In effective and efficient network, a smaller delay time is a better. Fig. 9 represents average delay time of our proposed authentication protocol.

The EPNR scheme has the smallest average of delay time compared to RSA and ACAFP schemes by comparison factor 0.046 and 0.285. It means that EPNR scheme can reduce delay time significantly. Table 5 shows the delay time of the proposed authentication protocol compared to the International Telecommunication Union standard [49].

From Table 5, our proposed authentication protocol based on EPNR has performance Excellent for key sizes (*800-3,200* bits), Good (*4,096-6,000* bits), and Poor (*7,000-8,192* bits) with no un-acceptable performance. It shows that the EPNR scheme is the best approach.

Authentication protocol models based on symmetric cryptosystem, such as in advanced AMI [17], smart grid [24], and WBAN [33], theoretically give higher throughput and smaller delay time. It is caused by faster processing in the symmetric cryptosystem [46]. Especially compared to smart city model that works based on RSA algorithm [38], our model is faster and theoretically give higher throughput and smaller delay time.

The third QoS parameter is packet loss rate. Packet loss rate means the rate at which packets are dropped, get lost, or become corrupted (some bits are changes in the packet) while going through the network. Our protocol works on Transmission Control Protocol/Internet Protocol (TCP/IP) scheme.

TCP/IP is communication protocol with connection-oriented. All of packet is guaranteed sent to the receiver. By the mechanism, packet loss in our experiments is 0 for all schemes.

6. Conclusion

In this paper, we have proposed a certificateless authentication protocol based on the EPNR method for single board computer environment implementation. The main advantage of the protocol is to speed up processing in client side without compromising the data security. Compared to previous models, the protocol is designed to simpler network and used one-time public-private keys. It also implements some secure mechanisms for anticipating statistical, replay, and MITM attack, such as ciphertext formatting in ASCII code, nonce/timestamp, and five-barrier data protections mechanism. The five-barrier data protections, includes hashing, first and second asymmetric encryption, blinding, and ASCII code format mechanism. It multi-barrier mechanism makes our model more secure from MITM attack compared to other models. As a protocol based on RSA cryptosystem, our model is better compared to the smart city model, in terms of random key generation, encryption, decryption, throughput, and delay time parameters. It is caused by EPNR method implementation.

A more comprehensive application of the double EPNR method as a communication protocol for distribution of secret keys and secure data transmission to support the RDMS in nuclear installation or radiation facility will be studied in the next researches.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Hermawan developed the concept, performed the computation simulation, and prepared initial manuscript. Winarko, Ashari, and Akhmad verified the method, supervised the findings of this works, evaluated and edited the manuscript draft. All authors discussed the results and contributed to the final manuscript.

Acknowledgments

This work was supported by Indonesian Nuclear Regulatory Agency that supported our research by the Indonesian Nuclear Regulatory Agency [memorandum of understanding numbers 01/KS 00 01/Set-PKS/II, 2016] scheme.

References

[1] IAEA, *Environmental and Source Monitoring for Purposes of Radiation Protection*, IAEA, Vienna, 2005.

[2] U.S. NRC, *Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities*, U.S. NRC, Washington, DC, 2010.

[3] N. T. E. Hermawan, E. Winarko, and A. Ashari, "Securing Data Transmission for Radiation Monitoring System in Nuclear Installation", *International Journal of Computer Application*, Vol. 179, No. 22, pp. 32–40, 2018.

[4] W. Stallings, *Cryptography and Network Security*, Seventh Ed, Pearson Prentice Hall, Singapore, 2017.

[5] I. T. Union, *Security Archhitecture for Open Systems Interconnection for CCITT Applications*, ITU, Geneva, 1991.

[6] S. Shaju, "BISC Authentication Algorithm : An Efficient New Authentication Algorithm Using Three Factor Authentication for Mobile Banking", In: *Proc. of International Conf. on Green Engineering and Technologies*, Coimbatore, India, pp. 1–5, 2016.

[7] D. Wang, G. S. Member, H. Cheng, D. He, and P. Wang, "On the Challenges in Designing Identity-Based Privacy-Preserving Authentication Schemes for Mobile Devices", *IEEE Systems Journal*, Vol. 12, No. 1, pp. 916–925, 2018.

[8] ISO/IEC, *Information Technology: Security Techniques - Entity Authentication (Part 1)*, Vol. 1, ISO/IEC, Geneva, 2010.

[9] Envinet, *Environmental Radiation Monitoring - SARA - Spectroscopic Radiation Detection*, Envinet GmbH, Munich, 2013.

[10] F. H. Al-naji and R. Zagrouba, "A survey on continuous authentication methods in Internet of Things environment", *Computer Communications*, Vol. 163, No. Sept, pp. 109–133, 2020.

[11] K. Philemon, K. Michael, and M. A. Shem, "Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system", *Journal of Medical Engineering & Technology*, Vol. 44, No. 1, pp. 12–19, 2020.

[12] S. Reinhardt, *SARA Spectroscopic Gamma Detector User Manual*, 1.8.0, Envinet GmbH, Munich, 2013.

[13] R. E. Hiromoto, A. Sachenko, V. Kochan, V.

Koval, V. Turchenko, O. Roshchupkin, V. Yatkiv, and K. Kovalak, "Mobile Ad Hoc Wireless Network for Pre and Post-Emergency Situations in Nuclear Power Plant", In: *Proc. of the 2nd IEEE International Symposium on Wireless Systems*, Ofenberg, Germany, pp. 92–96, 2014.

[14] J. Ebenezer and S. A. V. S. Murty, "Deployment of Wireless Sensor Network for Radiation Monitoring", In: *Proc. of 2015 International Conf. on Computing and Networks Communications (CoCoNet'15)*, Trivandum, India, pp. 27–32, 2015.

[15] A. Tocchi, V. Roca, L. Angrisani, F. Bonavolonta, and R. S. Lo Moriello, "First step towards an IoT implementation of a wireless sensors network for environmental radiation monitoring", In: *Proc. of IEEE International Conf. on Instrumentation and Measurement Technology*, Turin, Italy, pp. 1–6, 2017.

[16] J. H. Elrefaei, H. Kunber, M. K. Shaat, A. H. Madian, and M. H. Saad, "Energy-efficient wireless sensor network for nuclear radiation detection", *Journal of Radiation Research Applied Sciences*, Vol. 12, No. 1, pp. 1–9, 2019.

[17] Y. Yan, R. Q. Hu, S. K. Das, H. Sharif, and Y. Qian, "An Efficient Security Protocol for Advanced Metering Infrastructure in Smart Grid", *IEEE Network*, Vol. 27, No. 4, pp. 64–71, 2013.

[18] F. Ye, Y. Qian, and R. Q. Hu, "A Security Protocol for Advanced Metering Infrastructure in Smart Grid", *IEEE Network*, Vol. 27, No. 4, pp. 64–71, 2013.

[19] Y. Kabalci, "A survey on smart metering and smart grid communication", *Renewable Sustainable Energy Review*, Vol. 57, No. 1, pp. 302–318, 2016.

[20] M. Cebe and K. Akkaya, "Communication-efficient certificate revocation management for Advanced Metering Infrastructure and IoT Integration", *Future Generation Computer Systems*, Vol. 115, No. 1, pp. 267–278, 2021.

[21] A. Hansen, J. Staggs, and S. Shenoi, "Security analysis of an advanced metering infrastructure", *International Journal of Critical Infrastructure Protection*, Vol. 18, No. Sept., pp. 3–19, 2017.

[22] V. Ford, A. Siraj, and M. A. Rahman, "Secure and efficient protection of consumer privacy in Advanced Metering Infrastructure supporting fine-grained data analysis", *Journal of Computer and System Sciences*, Vol. 83, No. 1, pp. 84–100, 2017.

[23] S. Fan, F. Yen, J. Guo, Y. Liang, G. Xu, X. Zhang, and Y. Qian, "A Security Protocol for Wireless Sensor Networks Designed for Monitoring Smart Grid Transmission Lines", in *Proc. of 23rd International Conf. on Computer Communication and Networks (ICCCN)*, Shanghai, China, 2014, pp. 1–7.

[24] X. Zhang, F. Ye, S. Fan, J. Guo, G. Xu, and Y. Qian, "An adaptive security protocol for a wireless sensor-based monitoring network in smart grid transmission lines", *Secure Communication Networks*, Vol. 9, No. 1, pp. 60–71, 2016.

[25] D. He, S. Chan, and M. Guizani, "Cyber Security Analysis and Protection of Wireless Sensor Networks for Smart Grid Monitoring", *IEEE Wireless Communication*, Vol. 24, No. 6, pp. 98–103, 2017.

[26] K. Mahmood, S. Ashraf, H. Naqvi, and S. Kumari, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication", *Future Generation Computer Systems*, Vol. 81, No. Apr, pp. 557–565, 2018.

[27] L. Deng and R. Gao, "Certificateless two-party authenticated key agreement scheme for smart grid", *Journal of Information Sciences*, Vol. 543, No. Jan, pp. 143–156, 2021.

[28] L. Zhang, L. Zhao, S. Yin, C. Chi, R. Liu, and Y. Zhang, "A lightweight authentication scheme with privacy protection for smart grid communications", *Future Generation Computer Systems*, Vol. 100, No. Nov, pp. 770–778, 2019.

[29] J. P. D. Comput, X. Li, F. Wu, S. Kumari, L. Xu, and A. Kumar, "A provably secure and anonymous message authentication scheme for smart grids", *Journal of Parallel Distributed Computing*, Vol. 132, No. Oct., pp. 242–249, 2019.

[30] K. Wu, R. Cheng, W. Cui, and W. Li, "A lightweight SM2-based security authentication scheme for smart grids", *Alexandria Eng. Journal*, Vol. 60, No. 1, pp. 435–446, 2020.

[31] D. Sadhukhan, S. Ray, and M. S. Obaidat, "A Secure and Privacy Preserving Lightweight Authentication Scheme for Smart-Grid Communication using Elliptic Curve Cryptography", *Journal of Systems Architecture*, Vol. in progres, pp. 1–39, 2020.

[32] O. Majeed, M. Zulqarnain, and T. Majeed, "Recent advancement in smart grid technology : Future prospects in the electrical power network", *Ain Shams Eng. Journal*, Vol. in progres, No. July, pp. 1–9, 2020.

[33] S. K. Shankar, A. S. Tomar, and G. K. Tak, "Secure Medical Data Transmission by using ECC with Mutual Authentication in WSNs", *Procedia Computer Sciences*, Vol. 70, No. 1, pp.

455–461, 2015.

[34] S. Ji, Z. Gui, T. Zhou, H. Yan, and J. Shen, "An Efficient and Certificateless Conditional Privacy-Preserving Authentication Scheme for Wireless Body Area Networks Big Data Services", *IEEE Access Journal*, Vol. 6, No. Nov., pp. 69603–69611, 2018.

[35] M. E. S. Saeed, Q. Y. Liu, G. Tian, B. Gao, and F. Li, "Remote Authentication Schemes for Wireless Body Area Networks Based on the Internet of Things", *IEEE Internet of Things Journal*, Vol. 5, No. 6, pp. 4926–4944, 2018.

[36] Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari, and M. K. Khan, "Efficient Certificateless Aggregate Signature With Conditional Privacy Preservation in IoV", *IEEE Systems Journal*, Vol. 25, No. Feb., pp. 1–12, 2020.

[37] J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, "An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks", *Information. Sciences*, Vol. 451, No. July, pp. 1–15, 2018.

[38] M. M. Rathore, A. Paul, A. Ahmad, N. Chilamkurti, W. Hong, and H. Seo, "Real-time secure communication for Smart City in high-speed Big Data environment", *Future Generation Computer Systems*, Vol. 83, No. June, pp. 638–652, 2018.

[39] P. Chaudhury, D. Susmita, R. Monpreet, D. Saurav, S. Jyotirmoy, M. Aditya, B. Sauvik, R. Saraswata, K.S. Mrinal, K. Sanjay, and D. Rupayan, "ACAFP : Asymmetric Key based Cryptographic Algorithm using Four Prime Numbers to Secure Message Communication . A Review on RSA Algorithm", in *Proc. of 8th Annual Industrial Automation and Electromechanical Engineering Conf.*, pp. 332–337, 2017.

[40] C. E. Shannon, "Communication Theory of Secrecy Systems", *Bell System Tech. Journal*, Vol. 28, No. 4, pp. 656–715, 1949.

[41] A. Teixeira, A. Matos, A. Souto, and L. Antunes, "Entropy measures vs. Kolmogorov complexity", *Entropy*, Vol. 13, No. 3, pp. 595–611, 2011.

[42] B. Pingle, A. Mairaj, and A. Y. Javaid, "Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use", in *Proc. of IEEE International Conf. on Electro Information Technology*, Bangkok, Thailand, pp. 192–197, 2018.

[43] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé, and P. Zimmermann, "New factorization and discrete logarithm record computations", *Tech. l'Ingenieur*, Vol. hal-030456, No. Des., pp. 1–18, 2020.

[44] J. Bl and A. May, "A Generalized Wiener Attack on RSA", *LNCS Spinger*, Vol. 2947, No. May, pp.1-13, 2001.

[45] D. Kumar and H. Singh, "A secure authentication protocol for wearable devices environment using ECC", *Journal on Infrastructure Security Appl.*, Vol. 47, No. Aug., pp. 8–15, 2019.

[46] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms : DES , 3DES, AES, RSA and Blowfish", *Procedia Computer Science*, 2016, Vol. 78, No. Dec., pp. 617–624.

[47] S. Haryadi, *Telecommunication Quality of Service Concept*, Vol. I, CV Lantip Safari Media, Bandung, 2016.

[48] ITU, *Quality of Service - Regulation Manual*, Tel. Dev. Bureaue (BDT), Geneva, 2017.

[49] ITU-T, *Transmission Systems and Media, Digital Systems and Networks*, Recomm. G.114, ITUT-Telecommunication Standardization Sector, Geneva, 2003.