International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.1 (2025) pp. 1420-1433
http://www.ijcesen.com

ISSN: 2149-9144

Review Article

Literature Review on Lightweight Authentication Algorithms in Remote Data Transfer

Kalyankumar Dasari [1*], K. Sahadevalah[2]

[1]Research scholar, Department of Computer Science & Engineering, JNTUK, Andhra Pradesh, India.
* **Corresponding Author Email:** dkkumar123@gmail.com - **ORCID:** 0009-0008-1886-7127

[2]Professor, Department of Computer Science & Engineering, JNTUK, Andhra Pradesh, India.
Email: ksd1868@jntucek.ac.in - **ORCID:** 0009-0000-7402-6113

Article Info:

DOI: 10.22399/ijcesen.954
Received : 21 November 2024
Accepted : 27 January 2025

Keywords :

Lightweight cryptography,
Authentication,
İntegrity,
Smart Devices application.

Abstract:

With Smart Devices emerging as a potentially game-changing technology in the future, it is anticipated that it will generate a massive volume of data that may be vulnerable to security vulnerabilities. Therefore, lightweight cryptography has been identified as one of the acceptable mechanisms for protecting Smart Devices applications from hackers. This is since lightweight cryptography is designed to fulfill security demands in hardware and software that are resource constrained. When it comes to building lightweight cryptography for Smart Devices applications, specifically for integrity and authentication algorithms, the purpose of this study is to conduct an analysis of the existing security requirements. There was a four-step approach that was utilized to adopt the Kitchenham systematic review method. In this investigation, the articles that were chosen for research were retrieved from four credible databases, and after meeting the selection criteria, 57 of them were declared appropriate for subsequent analysis. A significant portion of the research was concentrated on assaults directed against Smart Devices applications, system security needs, and techniques for lightweight authentication. For the purpose of achieving the desired security requirements for sustainable security management in Smart Devices, this study may provide researchers with a reference for building user authentication algorithms that are lightweight.

1. Introduction

In the cutting-edge idea known as the Smart Devices, commonplace items like home and business appliances are connected to the web and may exchange data and instructions with one another. As a result, RFID tags, cell phones, smart environments, and other wearable tech can all be directly integrated [1]. Smart cities, healthcare, environmental surveillance, intelligent transportation systems, and military relations are some of the application sectors that have been rapidly developing thanks to the Smart Devices [2] According [3] over one billion smart objects, including sensors, actuators, GPS devices, mobile phones, and more, were anticipated to be connected to the Internet in 2020. Smart Devices has seen a meteoric rise in the number of devices connected to public networks, and these systems are constantly exchanging data with one another to reflect the actual environment. According to [4], the data is collected from authorized users and transmitted to terminal nodes using a wireless network. Data storage and transmission to the central platform are responsibilities of the terminal nodes. Cyber-attacks can penetrate these several levels of the communication process if a security system is not put in place [5]. Therefore, to guarantee the security of data during connection, mutual authentication is essential. The security of Smart Devices relies heavily on mutual authentication. An unsecured perimeter leaves nodes vulnerable to distant users employing hacking tools [6]. Specific nodes can have their unique information extracted after they are coupled. Deploying resourceful gateway nodes in Smart Devices networks will boost system efficiency in terms of processing capacity, battery backup, memory, speed, and other aspects, which is why remote-user authentication is crucial [7]. In comparison to conventional wired networks, the design, features, and uses of the Smart Devices are unique. Devices with limited resources cannot use traditional encryption methods. Lightweight algorithms have thus become one of the most effective ways to encrypt data in these devices without significantly increasing their power consumption [8].

Protecting the information necessary for the Smart Devices to function requires the use of cryptography in smart devices. This is to make sure that only the devices that are meant to receive the data can access it during wireless transmission. An encryption algorithm can be employed to code and decode the data, ensuring its security [9]. Although encryption can be employed to guarantee data authenticity and integrity, conventional cryptography methods necessitate substantial resource allocation. Since Smart Devices have limited resources like processing power, memory, and battery life, new methods of network security are needed [10]. In response to these constraints, lightweight cryptography was developed to oversee the protection of devices with little resources. In addition to protecting data, lightweight cryptography keeps memory and power consumption in Smart Devices to a minimum [11]. Hospitals employ Smart Health, sometimes called e-health, as an example of lightweight cryptography technology that has been extensively studied. Electronic health records allow for continuous monitoring of a patient's status. Secure transmission of patient data between e-health devices is, hence, of the utmost importance [12]. Even when they aren't on the clock, doctors may find value in reading patients' medical records. Insecure hospital Smart Devices systems leave patients vulnerable to hackers who could take control of their devices, alter the data they collect, and even steal patient information. There is a risk that patients could suffer harm due to treatment delays or errors caused by altered or compromised data.

One way to lessen the likelihood of data privacy breaches in Smart Devices applications is to use lightweight cryptography. Data interchange over the Internet is the initial step in Smart Devices. Hackers often aim their attacks at this weak point in the system. The data transmitted by a certain endpoint might not be a cause for worry in terms of privacy on its own. Yet, when collected, processed, and analysed, incomplete data from several sources might reveal confidential information. Following a systematic literature review (SLR) defined by [13] as "a means of identifying, evaluating and interpreting all available research relevant to a particular research question or topic area or phenomenon of interest," this paper reviews the lightweight authentication algorithm. Due to its evidence-based nature and the superiority of its results over subjective opinions or casual observations, a systematic review has gained widespread recognition and application outside of software engineering and medical research [14]. To gain people's trust in the Smart Devices, which will soon be the standard, a solid security system is required. Therefore, it is essential that every Smart Devices device has a unique identifier that can be checked whenever it attempts to establish a connection to a hub or main server. Keeping tabs on every device that connects to a system is crucial for IT system administrators. Consequently, this study aims to:

(1) Assess the existing research on integrity and authentication for lightweight algorithms in Smart Devices applications.

(2) Investigate the algorithms' needs for integrity and authentication and

(3) Examine the algorithms that are currently being used. Possible uses of the findings from this study include:

(a) Improving existing lightweight algorithms

(b) Outlining appropriate safety standards for lightweight algorithms and

(c) Analyzing the merits and shortcomings of prior research on these algorithms

2. Material and Methods

Figure 1 depicts the review process. Making a list of potential research topics was the first step. Next, using inclusion-exclusion criteria, we searched for publications that provided details on the publications' selection process as well as keywords. The last step was to compile a list based on the extracted information from the chosen articles.

2.1 Formulation of Research Questions

Tabulated in Table 1 are the research questions (RQ). When it came to RQ1, the question aimed to provide an overview of the current research trend on the security of Smart Devices applications using a lightweight authentication mechanism. The number of journals and conferences that published papers between 2013 and 2021 was determined in order to answer RQ1. Research Questions 2 and 3 looked at the present state of lightweight algorithms utilized in Smart Devices applications and the requirements for their integrity and authentication.

2.2 Search Process

The hunt is the most important part of an SLR. As shown in Figure 2, the following databases were searched for English-language articles in seven stages:

- Google Scholar
- Scopus
- Springer/Elsevier

- IEEE Digital Library

The search method is illustrated in Figure 2. Beginning with a broad literature search utilizing terms such as "authentication," "integrity," "Smart Devices application," and "lightweight cryptography," the second phase involved more specific searches. Phase 2 involved downloading all papers that had the keywords in the title and abstract. After the third phase, which involved reading all of the downloaded materials, the articles were organized by topic, including security, architecture, and algorithms. After selecting 52 articles in Phase 3, the following phases narrowed the search using synonyms of keywords from Phase 1 (e.g., "authentication" was changed to "verification"). Following these steps, five articles were identified that were similar to the synonyms used in the SLR.

2.3 Inclusion and Exclusion Criteria

Articles were reviewed in Phase 6 for inclusion and exclusion criteria before they were accepted as main articles. Papers were selected for primary analysis based on the inclusion criteria listed in Table 2. Afterwards, items that did not meet the criteria outlined in Table 3 were not included.

3. Results and Discussions

Consistently obtaining outcomes to answer the review questions was the purpose of data extraction following final article selection in Phase 7.

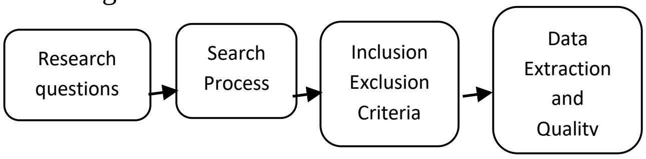

Figure 1. *The steps of the SLR described by Kitchenham et al. (2004) [39]*

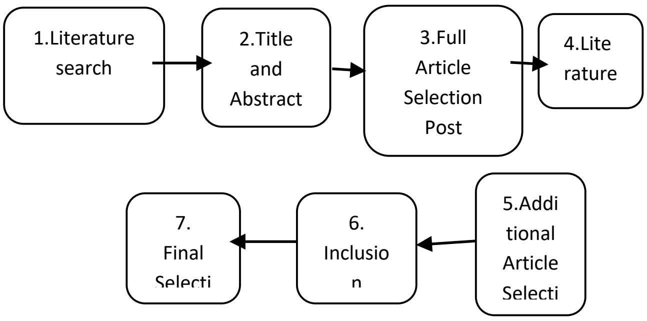

Figure 2. *Search process of SLR*

To accurately and fairly collect data from chosen articles, a data extraction form needs to be filled out. In accordance with the quality assessment standards employed by [15,16] five criteria were listed in Table 4 to determine the quality of the chosen articles. Various ratio scales were employed: One point for yes, zero for no, and half a point for partially.

3.1 Data Extraction and Quality Assessment

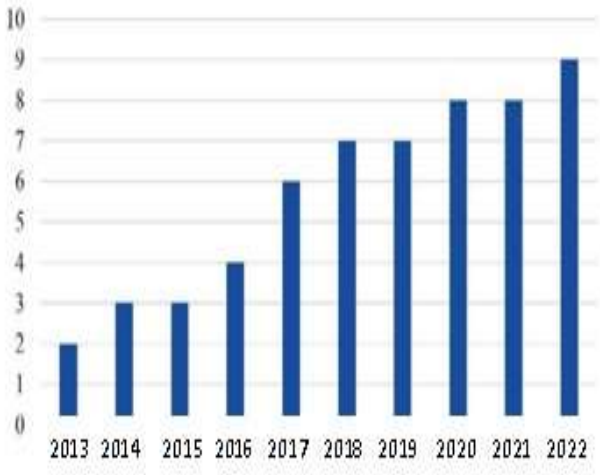

Figure 3. *Numbers of articles after inclusion and exclusion criteria (2011-2022)*

The results of the SLR are given here. Table 1's research questions were addressed in each subsection.

Question 1: How is the state of the art in the field of authentication and integrity algorithms for Smart Devices applications?

The quantity of publications provided between 2013 and 2022 prior to the quality assessment is depicted in Figure 3. Lightweight authentication in Smart Devices apps was not a top concern between 2013 and 2014, as shown in the figure. In 2015 and beyond, the quantity of publications skyrocketed due to the widespread use and decreasing prices of smart devices [17]. Also, studies on lightweight algorithms were in their infancy between 2013 – 2014. Potential threats to Smart Devices applications, necessary security measures to safeguard these applications, and recommended algorithms constituted the bulk of the article content. As shown in Figure 3, a total of 103 articles were located using the following keywords: lightweight cryptography, authentication, integrity, and Smart Devices applications. A total of 109 papers met the criteria set out by the keywords. After careful selection utilizing the inclusion-exclusion criteria and quality assessments shown in Tables 2, 3, and 4, a total of 57 articles were obtained. Of these, 52 were in the first search, and the remaining five were selected from the second search using the phrase "verification." Figure 4 is a pie chart displaying the total number of publications categorized as follows: assaults, security methods, and algorithms; these are the three main areas of Smart Devices security.

There were 18 pieces dealing with assaults, 26 with security needs and procedures, and 13 with lightweight cryptographic algorithms. Reading up on authentication and integrity-related articles about Smart Devices vulnerabilities helped shed light on how light weight cryptography protected Smart Devices systems. To identify security holes in Smart Devices applications and the measures to close them, these attacks could be used. Moreover, security requirements have shown how critical it is to enforce security regulations in Smart Devices systems. We could construct the appropriate algorithms when we had determined the security requirements.

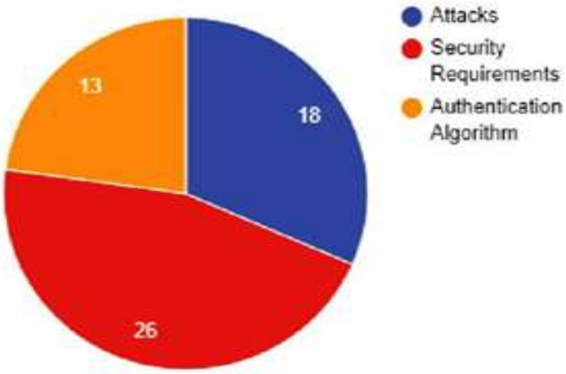

Figure 4. *Classification of articles (2011 to 2023)*

3.2 Research Question 1.1: Which threats could compromise the security of Smart Devices applications?

Smart Devices has been the target of several assaults. Applications' credibility and security would be the primary targets of the assaults discussed in this article. Based on an examination of the 52 main articles, many occurrences included spoofing, data manipulation, side-channel attacks, unauthorized access, hash collision, and man-in-the-middle (MIM) attacks. Eighteen of the main papers addressed the assaults that posed a risk to the security of apps built for the Smart Devices. Here is a summary of the publications that covered the specific assaults and how they worked (Table 5).

It appeared that most often, hackers would launch MIM assaults, in which they would hijack the data flow that goes between devices and cloud-based services. Based on previous research [19,20] it is possible for a hacker to intercept and manipulate data transmissions across systems. Given that the scale of harm may range from negligible to massive, depending on the hackers' intentions, MIM posed a real danger to Smart Devices applications. Smart Devices applications are vulnerable to this type of vulnerability attack, particularly if the authentication measures were inadequate. In addition, an attacker could be able to obtain login passwords and personal information using MIM. Because a hacker may execute fraudulent outputs by sending command-and-control instructions to insecure Smart Devices applications, MIM assaults would be encouraged. A strong client-server encryption technique was employed by [21] to address MIM attacks. After the server verified the client's request using a digital certificate, the connection could be formed. According to [22] the danger of unauthorized access and sensitive data leaks will develop in direct proportion to the number of interconnected links between data sources and Smart Devices applications. This kind of assault happened when incomplete data identification was the outcome of intercepting and cross-referencing many data sources [23]. Hackers could use the stolen information without affecting the Smart Devices apps directly. Worst case scenario: unauthorized access leads to data and information leakage. The security of Smart Devices applications might be jeopardized if hackers could alter, delete, or copy data. According to one of the most effective ways to protect data kept on a physical server or in the cloud against unauthorized access is to use physical security measures. Security measures may include the use of guards, physical barriers, closed-circuit television, and locks for computers and other devices. It is also a good idea to combine physical security measures with Smart Devices technology when using connected sensors and actuators [21]. According to [22], data manipulation takes place when records are altered because of hacking. According to [23], once hackers intercept or access data, they would alter the material for their own benefit. Two instances of data alteration were taking advantage of deficient security measures (such as tiny or weak passwords) and exploiting numerous vulnerabilities in Smart Devices apps (such as SQL injection and cross-site scripting) [23,24] found that encrypted storage methods could prevent data breaches in the Smart Devices. The Shamir Secret Sharing method was one cryptographic-based storage strategy that could securely store aggregated data from the Smart Devices in an object [25]. Long-term security for Smart Devices data can be achieved without the requirement for encryption using non-cryptographic-based approaches like POTSHARDS [26]. The method's security rested on distributing data among several storage servers after dividing it into numerous pieces, each with its own pointer. The attacker faced a significant challenge in retrieving data from individual segments because to the dispersed nature of the segment pointers, which were difficult to get [27]. According to [28], a side-channel attack is based on discovering information by analysing accessible side aspects of an algorithmic implementation, such as process timing, power usage, and even accompanying sounds. An insecure method of processing and storing data on the Smart Devices, such as leaving data unencrypted in the cloud or on Smart Devices apps, might lead to this kind of assault. 10] discussed data leakage attacks against Cascading Style Sheets (CSS), including file confirmation and comprehending the content of files.

File confirmation might be used by an attacker who knew the file's plaintext content to find out if a copy had been saved somewhere else in the CSS [29]. Since the hacker was already familiar with most of the file's contents, he could potentially gain access to sensitive information by deciphering it using techniques like comparing the encrypted output to the deciphered cipher text [20]. Using temporary data storage was one of the methods to reduce the impact of side-channel attacks. One definition of transient data storage is the capacity to retain or delete data once a system has finished processing it. However, management of transient Smart Devices data generated during system execution has only been the subject of a few research [21]. Data processing during system execution would create new copies of data that users might save or remove according to their requirements; here is where transient data would become significant [20]. advantage of deficient security measures (such as tiny or weak passwords) and exploiting numerous vulnerabilities in Smart Devices apps (such as SQL injection and cross-site scripting) [51-74].

Yu and Guo (2016) found that encrypted storage methods could prevent data breaches in the Smart Devices [75]. The Shamir Secret Sharing method was one cryptographic-based storage strategy that could securely store aggregated data from the Smart Devices in an object [68]. Long-term security for Smart Devices data can be achieved without the requirement for encryption using non-cryptographic-based approaches like POTSHARDS [56]. The method's security rested on distributing data among several storage servers after dividing it into numerous pieces, each with its own pointer. The attacker faced a significant challenge in retrieving data from individual segments because to

Table 1. *Three research questions to address in this study*

No.	Details
RQ1	1. What is the current research trend in integrity and authentication algorithms of Smart Devices applications? 1.1 What are the attacks that can jeopardize the integrity of Smart Devices applications?
RQ2	2. What are the security requirements and mechanisms needed to resolve integrity and authentication attacks?
RQ3	3. Which lightweight algorithm is suitable to achieve integrity requirements in Smart Devices?

Table 2. *Criteria used in accepting searched articles*

S.NO:	**Authors**	**Attacks**	**Mechanism**
1	[49]	Man-in-the- middle attack	The hacker intercepts a communication between two systems and tricks the recipient into thinking they are still getting a legitimate message.
2	[18]		
3	[29]		
4	[37]		
5	[20]		
6	[10]		
7	[7]		
8	[5]		
9	[21]		
10	[29]		

Table 3. *Criteria used in excluding searched articles*

S.NO:	**Authors**	**Attacks**	**Mechanism**
1	[42]	Linkage attack	The hacker manipulates the intercepted \data without interfering with the actual Smart Devices applications, stealing critical information in the process recipient into thinking they are still getting a legitimate message
2	[51]		
3	[20]		

Table 4. *Data extraction and quality assessment*

Item	Answer
QA1: Was the article peer-reviewed?	Yes/No
QA2: Was there a clear statement of the objectives?	Yes/No/ Partially
QA3: Was there adequate description of the context in which the research was	Yes/No/ Partially
carried out? For example, did it clearly state the problems that led to the research,	
descriptions of research methodology used, etc.	
QA4: Was the data collection performed thoroughly? For example, did the evaluation	Yes/No/ Partially
of the proposed approach answer the research questions? did the article provide a	
thorough discussion of results?	
QA5: Was the simulation results rigorously analyzed?	Yes/No/ Partially

the dispersed nature of the segment pointers, which were difficult to get [5].

According to Harnik et al. (2016), a side-channel attack is based on discovering information by analyzing accessible side aspects of an algorithmic implementation, such as process timing, power usage, and even accompanying sounds [33]. An insecure method of processing and storing data on the Smart Devices, such as leaving data unencrypted in the cloud or on Smart Devices apps, might lead to this kind of assault. Aleisa and Renaud (2017) discussed data leakage attacks against Cascading Style Sheets (CSS), including file confirmation and comprehending the content of files [10].

File confirmation might be used by an attacker who knew the file's plaintext content to find out if a copy had been saved somewhere else in the CSS [5]. Since the hacker was already familiar with most of the file's contents, he could potentially gain access to sensitive information by deciphering it using techniques like comparing the encrypted output to the deciphered cipher text [20].

Using temporary data storage was one of the methods to reduce the impact of side-channel attacks. One definition of transient data storage is the capacity to retain or delete data once a system has finished processing it. However, management of transient Smart Devices data generated during system execution has only been the subject of a few of research [33]. Data processing during system execution would create new copies of data that users might save or remove according to their requirements; here is where transient data would become significant [20]. A hacker commits spoofing when he or she gains unauthorized access to a system by masquerading as a legitimate user. Smart Devices devices are tricked into thinking the data came from a trusted source when in fact it was being sent by the hacker. Because of this, the gadgets would be completely susceptible to the attacker's control [34]. An assault known as "replacing" involves using a second "duplicate call" to mimic previously authorized commands [42]. The receiver could be tricked into performing the hacker's bidding if the data was captured during a secure network communication utilized by Smart Devices, fraudulently delayed, or reissued. [43] noted that replay attacks pose an additional risk because, once

Table 5. *Articles that discuss attacks on the integrity of Smart Devices applications*

S.No	Authors	Attacks	Mechanism
1	[50]	Man-in-the-middle attack	The hacker intercepts communication between two systems and tricks the recipient into thinking they are still getting a legitimate message
2	[18]		
3	[29]		
4	[37]		
5	[20]		
6	[10]		
7	[7]		
8	[5]		
9	[21]		

they get a message from Smart Devices and networks, hackers do not even require specialized expertise to decipher it.

3.3 Question 2: How can we prevent and deal with assaults on authentication and integrity? What are the necessary security measures?

Attacks on the integrity of Smart Devices applications are addressed in this section, along with the security requirements and procedures to resolve them. Security needs and processes are covered in 21 articles. Articles discussing the need for security in Smart Devices applications are listed in Table 6. Five authentication and integrity-related security criteria have been identified from the articles. The necessity to set up authentication mechanisms and their role in maintaining security rules were both laid forth in these standards.

The restricted nature of gadgets should be considered when developing lightweight solutions. According to [66], the applications' ability to implement cryptographic algorithms and protocols could be hindered by computational limitations. Lightweight security systems need to find a happy medium between power needs and device battery capacities in order to optimize energy use. An efficient security method with low memory and power consumption and fast command execution is required for Smart Devices applications. Finally, end-to-end security is another practical consideration. The Smart Devices would use a maze of administrative domains for communication. According to it is essential to ensure security across the entire relationship, including safe storage, communication, content, authentication, and system integrity [27]. Concerns about user data and information exposure in a Smart Devices setting arise when the scope and character of the Smart Devices call for a unique emphasis on privacy concerns [19]. Verification of identity and anonymity is necessary for Smart Devices applications, whether at the device or aggregate level. Reliable methods of managing user and device identities, along with the capability to handle connections between these identities in a flexible way, are essential components of security [9]. A few examples of what was involved were the adaptable support for identity management and mutual authentication for users, devices, applications, and related services, and the smooth integration of varied services across several domains to connect various users and devices. According to Sharma et al. (2018), security solutions should take into account the fact that knowing everyone involved in an interaction isn't always feasible [60]. This will help them handle the large number of identities in the system. Due to the scalability problem, identity management became more cumbersome and often involved using a single identity to represent multiple entities [29]. Although identification is often considered a basic security measure, the sheer scale of the Smart Devices would call for creative approaches to identity management. Authentication was an area where this requirement really shone through, allowing various users of Smart Devices applications to be verified through login credentials, biometric data, and RFID tags. Given the mobility of its constituent parts, the Smart Devices has the potential to perform extraordinarily well on a massive scale. As a result, needs for mobility were identified, these systems need to be very dynamic [62]. Three broad types of mobility exist: location privacy, dynamic infrastructure, and numerous jurisdictions. Data transmission routing would be crucial due to the resource-constrained and dynamic topology of Smart Devices. According to Deep et al. (2019), most Smart Devices nodes may connect through any network, not just the Internet [25].

Table 6. *Articles that discuss attacks on the integrity of Smart Devices applications*

	Authors	**Attacks**	**Mechanism**
1	[42]	Linkage attack	The hacker manipulates the intercepted data without interfering with the actual Smart Devices applications, stealing critical information in the process
2	[51]		
3	[20]		

Table 7. *Articles that discuss attacks on the integrity of Smart Devices applications*

	Authors	Mechanism
1	Roman et al. (2013) [56]	Data Using SQL injection and cross-site manipulation scripting, the hacker attacks Smart Devices apps directly
2	Williams et al. (2016) [68]	
3	Yu and Guo (2016) [73]	
4	Abdulghani et al. (2019) [5]	
5	Grobauer et al. (2013) [29]	
6	Miorandi et al. (2016) [51]	

Table 8. *Studies on security requirements for Smart Devices applications*

S.NO	Authors	Security Requirements	Description
1	[12]	Lightweight mechanism	Light-weight security mechanisms must be designed with device limitations in mind such as energy consumption, limited memory and computational processing
2	[8]		
3	[30]		
4	[24]		
5	[31]		
6	[6]	End-to-end security	Provisioning for secure storage, authentication and integrity must be ensured for communication
7	[27]		
8	[28]		
9	[19]		
1	[15]	Privacy	Users want to keep their personal information private while getting the services they need
2	[71]		
3	[72]		
4	[32]		
5	[29]		
1	[9]	Identity management	Authentication helps to identify users which can be performed through the login of username, biometrics, etc.
2	[20]		
3	[29]		
4	[60]		
5	[62]	Mobility	Mobility requires the ability to accelerate tendencies for the device to provide

This included Wireless Sensor Networks (WSN), Wireless Local Area Networks (WLANs), and Personal Area Networks (PANs). The degree to which structure, location, and architecture vary in a real-time environment must be considered by the security approach. In order to make it easier for linked devices, users, and things to move around, security solutions were needed that could let data flow freely across different jurisdictions [52]. A database's syncing capabilities with mobile devices allow for precise execution of data regardless of location, thanks to mobility [25]. It was necessary to incorporate a security mechanism into every layer of the Smart Devices architecture. Our goal is to ensure that every layer is protected with security measures, making it impossible for any assaults to occur within that layer. To see how each layer of the Smart Devices handles security (Table 7). Table 8 is studies on security requirements for smart devices applications and table 9 is smart devices layers concerning security mechanism. The perception and network layers are vulnerable to MIM attacks, as shown in Table 7. All three of these levels, plus the application layer, are vulnerable to unauthorized access, not only in MIM. Therefore, these two levels must implement privacy protection through end-to-end authorization in order to counter this attack.

Table 9. *Smart Devices layers concerning security mechanism*

Authors	Smart Devices Layer	Authentication Algorithm	Attacks	Security Mechanism
[63]	Application	Multiple authentications using physical context	Data manipulation, spoofing	Authentication
[43]	Perceptual, network and application	Privacy-preserving using ECC	Unauthorised access	Privacy protection
[53]	Network and perceptual	Authentication and key management using entity ID and serial number	A man-in-the-middle attack, unauthorised access	Intrusion detection system Privacy protection
[58]	Perceptual, network and application	Two-way authentication using RSA and ECC	Data manipulation	Authentication key management
[72]	Network and perceptual	Access control using ECC	Spoofing	Access control mechanisms

Because of the potential for data tampering and spoofing at the perception, network, and application layers, authentication key management had to be put in place. Table 9 shows that in order to safeguard the Smart Devices system and its applications from assaults, a robust authentication technique had to be implemented.

3.4 Research Question 3: Which efficient algorithm can meet the integrity standards of the Smart Devices?

The authors' emphasis on the authentication and integrity of Smart Devices applications led to the proposal of numerous lightweight techniques. The algorithms were examined to identify the advantages and disadvantages of the Smart Devices. Intelligent service security was defined in relation to application protocols. The capabilities of Smart Devices applications were enhanced through the combination of cross-platform communication, encryption, signature, and authentication. In contrast, the Datagram Transport Layer Security (DTLS) protocol, developed by [41], is situated between the transport and application layers and offers two-way authentication protection. It is based on RSA and was optimized for IPv6 over Low Power Wireless Personal Area Networks (6LoWPANs). In addition, OCARI, an optimization of communication for ad hoc reliable industrial networks, was the subject of proposal for a strong shared authentication protocol for WSNs. OCARI suggested that all nodes that want to connect to the network should be authenticated at the OCARI MAC sub-layer.

Using hash protocols,[66] presented a polynomial scheme that includes two appropriate key management systems. The algorithm could protect against MIM attacks and manage authentication.[69] later suggested a signature-encryption strategy for transmission, which met the needs for Smart Devices security by way of Object Naming Service (ONS) queries. Users' and the system's data integrity, trustworthiness of the network, and identity verification were all guaranteed. For Smart Devices with low processing power and memory, developed an authentication protocol that protected user privacy and prevented spoofing by using lightweight encryption that relied only on XOR manipulation. Finally, for the purpose of controlling user access,[72] suggested an authentication encryption method based on Elliptic Curve Cryptography (ECC).

Elliptic Curve Lightweight Cryptography (ECLC) was suggested by [44] to protect data transmitted by the Smart Devices utilizing key agreements. The ECLC enabled WSN nodes to establish connections with one another while consuming little resources in terms of processing and storage. The authors suggested ECLC as a solution for MANET because of the advantages of its small key size and low cost. Compared to other cryptosystems like RSA, MANET's key size is significantly cheaper, which means reduced memory needs, less bandwidth utilization during key exchange over the communication channel, and easier data administration. Comparing ECC with other public key cryptography methods, we find that their computation costs are lower. According to [38], this method was expected to prolong the lifetime of the network, in contrast to other algorithms that rely on exponentiation. These other algorithms could cause all nodes' power budgets to be used early in the network's layers.

To secure the authenticity and integrity of Smart Devices applications, prior publications have suggested authentication techniques that use hybrid solution algorithms (Table 10). There were benefits to using these algorithms to achieve the goals, but there were also drawbacks that could compromise the security of Smart Devices systems.

4. Conclusions

We set out to accomplish three things with this paper. The first goal was to assess where the lightweight algorithm's integrity and authentication research stands now. It was found in the reviewed articles that there were still Smart Devices applications with authentication and integrity concerns. Data breaches involving electronic health records (EHRs) have been reported [24]. These records may include personal information, financial details, and medical history. Security researchers have identified and described vulnerabilities such MIM assaults, data manipulation, and spoofing that disturb the integrity of applications; these attacks can be used to analyze the integrity of the Smart Devices. Examining the authenticity and integrity needs of Smart Devices applications was the secondary goal. In this piece, authentication and integrity were highlighted as the primary security requirements. Lightweight solutions, privacy, end-to-end security, identity management, and mobility were all among them. Authentication and integrity protocols for Smart Devices applications, as well as security mechanisms for these applications, were also covered. Finally, the study of lightweight algorithms and schemes was conducted to accomplish the intended design need for authentication in Smart

***Table 10.** Authentication schemes for Smart Devices*

Author	Smart Devices Layer	Algorithm	Strength	Weakness
[70]	Application	Context/multiple credentials using physical context	Packet encapsulation to reduce the overhead of data resources	DoS attack is not considered
[38]	Network and perception	Assymmetric encryption using ECC	The cost of ECC computation is lower than that of other public key cryptography techniques	Vulnerable to side channel attacks
[41]	Application and network	Encryption/ asymmetric using RSA	Low overhead and high interoperability	Using UDP over DTLS leads to unreliable authentication
[32]	Perception	Encryption/ symmetric asynchronous one time password (OTP)	Resistant to replay and some DoS attacks	No performance measurement done in comparison with other schemes
[69]	Application, network and perception	Encryption using AES symmetric	Resilient to attacks, data confidentiality, access control and client privacy	Location privacy is not considered
[45]	Network and perception	Encryption/ symmetric using XOR	Authentication of RFID tags with readers	Location privacy is not considered
[44]	Network and perception	Encryption using ECC known as ECLC	Achieve greater efficiency and flexibility than the aforementioned alternatives. They have been adopted in a wide range of applications and in some cases, under critical constraints	ECLC must observe the lengthy latencies and the hardware/processing overhead compared with symmetric lightweight cryptography
[66]	Network and perception	Encryption/ symmetric + hash	Resistant to replay attacks, man-in-the-middle attacks, impersonation attacks, privileged insider attacks, stolen smart card attacks and smart card breach attacks	Communication cost is higher than other schemes
[72]	Network and perception	Encryption/ asymmetric using ECC	Resistant to DoS, replay attack, eavesdropping, node capture and man-in-the-middle attacks	Brief discussion related to attribute-based access control

Devices applications. According to Ye et al. (2014), there was a significant lack of studies on ECC adoption [72]. Despite its potential inefficiency, this approach was manageable and could satisfy authentication security standards.

In conclusion, more and more problems will arise due to the exponential growth of wireless technology. Developers and designers of systems for the Smart Devices are encouraged to use this SLR as a guide for dealing with authentication and integrity concerns.

In this piece, authentication and integrity were highlighted as the primary security requirements. Lightweight solutions, privacy, end-to-end security, identity management, and mobility were all among them. Authentication and integrity protocols for Smart Devices applications, as well as security mechanisms for these applications, were also covered. Finally, the study of lightweight algorithms and schemes was conducted to accomplish the intended design need for authentication in Smart

Devices applications. According to Ye et al. (2014), there was a significant lack of studies on ECC adoption [72]. Despite its potential inefficiency, this approach was manageable and could satisfy authentication security standards.

In conclusion, more and more problems will arise due to the exponential growth of wireless technology. Developers and designers of systems for the Smart Devices are encouraged to use this SLR as a guide for dealing with authentication and integrity concerns.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Adnan Sohail, Abdul Hameed, Muhammad Farhan, Faiz Abdullah Alotaibi, And Mrim M. Alnfiai. (2023). Robust and Lightweight Remote User Authentication Mechanism for Next-Generation IoT-based Smart Home. *IEEE Transations*. 11: 137899-
137910. DOI:10.1109/ACCESS.2023.3336763

[2] Sangjukta Das Patna, Maheshwari Prasad Singh , m Suyel Namasudra. (2023, July 14-16). A Lightweight Authentication and Key Agreement Protocol for IoT-based Smart Healthcare System. *2023 World Conference on Communication & Computing (WCONF) Raipur, India.*

[3] Sanaz Kavianpour Abdul Razaq Gavin Hales. (2023, 19-20 July). A secure lightweight authentication mechanism for IoT devices in generic domain. *Proc. of the International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME 2023). Tenerife, Canary Islands, Spain.*

[4] B.D. Deebak, Fadi AL-Turjman. (2023). Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing. *Future Generation Computer Systems*. 116:406-425. DOI:10.1016/j.future.2020.11.010

[5] Abdulghani, H. A., Nijdam, N. A., Collen, A., Konstantas, D. (2019). A study on security and privacy guidelines, countermeasures, threats: Smart Devices Data at rest perspective. *Symmetry*. 11(6):774. DOI: 10.3390/sym11060774.

[6] Ahanger, T. A., Aljumah, A. (2019). Smart Devices: A comprehensive study of security issues and defense mechanisms. *IEEE Access*. 7:11020-11028. DOI: 10.1109/ access.2018.2876939.

[7] Ahmed, A., Latif, R., Latif, S., Abbas, H., Khan, F. A. (2018). Malicious insiders attack in Smart Devices based Multi-Cloud e-Healthcare environment: A systematic literature review. *Multimedia Tools and Applications*. 77(17):21947-21965. DOI: 10.1007/s11042-017-5540-x.

[8] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M. (2015). Smart Devices: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*. 17(4):2347-2376. DOI: 10.1109/ comst.2015.2444095.

[9] Alam, S., Siddiqui, S. T., Ahmad, A., Ahmad., R., Shuaib, M. (2020). Smart Devices enabling technologies, requirements, and security challenges. *In Advances in data and information sciences*. 119-126. *Berlin/Heidelberg, Germany: Springer.*

[10] Aleisa, N., Renaud, K. (2017). Privacy of the Smart Devices: A systematic literature review. *Proceedings of the 50th Hawaii International Conference on System Sciences*. DOI: 10.24251/ hicss.2017.717

[11] Almulhim, M., Islam, N., Zaman, N. (2019). A lightweight and secure authentication scheme for Smart Devices based e-health applications. *International Journal of Computer Science and Network Security*. 19(1):107-120.

[12] Aswale, P., Shukla, A., Bharati, P., Bharambe, S., Palve, S. (2019). An overview of Smart Devices: Architecture, protocols and challenges. *In Information and communication technology for Intelligent Systems*. 299-308. *Berlin/Heidelberg, Germany: Springer.*

[13] Azni, A. H., Ahmad, R., Noh, Z. (2013). Survivability modeling and analysis of mobile ad hoc network with correlated node behavior. *Procedia Engineering*. 53:435-440. DOI:10.1016/j.proeng.2013.02.057

[14] Azni, A. H., Ahmad, R., Noh, Z. A. M., Hazwani, F., Hayaati, N. (2015). Systematic review for network survivability analysis in MANETS. *Procedia-Social and Behavioral Sciences*. 195:1872-1881. DOI:10.1016/j.sbspro.2015.06.424

[15] Bansal, S., Kumar, D. (2020). Smart Devices Ecosystem:A survey on devices, gateways, operating systems. Middleware and Communication. *International Journal of Wireless Information Networks*. 27(4):1-25. DOI:10.1007/s10776-020-00483-7

[16] Blackburn, S. R., Robshaw, M. J. (2016). On the security of the Algebraic Eraser Tag Authentication Protocol. *Applied Cryptography and Network Security Lecture Notes in Computer Science*. 3-17. DOI: 10.1007/978-3-319-39555-5_1

[17] Bösch, C., Guajardo, J., Sadeghi, A., Shokrollahi, J., Tuyls, P. (2008). Efficient Helper Data Key Extractor on FPGAs. Cryptographic Hardware and Embedded Systems– *CHES 2008 Lecture Notes in Computer Science*. 181-197. DOI: 10.1007/978-3-540-85053-3_12

[18] Brinkmann, A., Fiehe, C., Litvina, A., Luck, I., Nagel, L., Narayanan, K., Ostermair, F., Thronicke, W. (2013). Scalable Monitoring System for Clouds. *In Proceedings of the 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing, Dresden, Germany*. 9-12.

[19] Cai, H., Xu, B., Jiang, L., Vasilakos, A.V. (2016). Smart Devices-based Big Data Storage Systems in Cloud Computing: Perspectives and challenges. *IEEE Internet Things Journal*. 4:75-87.

[20] Cherdantseva, Y., Hilton, J. (2013). A reference model of information assurance and security. *2013 International Conference on Availability, Reliability and Security*. DOI: 10.1109/ares.2013.72

[21] Claycomb, W. R., Nicoll, A. (2012). Insider threats to Cloud Computing: Directions for new research challenges. *2012 IEEE 36th Annual Computer Software and Applications Conference*. DOI: 10.1109/ compsac.2012.113

[22] Columbus, L. (2017, December 11). 2017 Roundup of Smart Devices Forecasts. Forbes. https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/?sh=3d933e2f 1480. Access on 15 May 2021.

[23] Das, A. K., Zeadally, S., He, D. (2018). Taxonomy and analysis of security protocols for Smart Devices. *Future Generation Computer System*. 89:110-125. DOI:10.1016/j.future.2018.06.027

[24] Davoli, L., Veltri, L., Ferrari, G., Amadei, U. (2019). Smart Devices on Power Line Communications: An experimental performance analysis. In Kabalci, E., Kabalci, Y., (Eds.), *Smart grids and their communication systems*. 465-498. *Singapore: Springer.*

[25] Deep, S., Zheng, X., Hamey, L. (2019). A survey of security and privacy issues in the Smart Devices from the layered context. *arXiv 2019*. arXiv: 1903.00846.

[26] Delvaux, J., Gu, D., Verbauwhede, I., Hiller, M., Yu, M. D. (2016). Efficient fuzzy extraction of PUF-Induced Secrets: Theory and applications. *Lecture Notes in Computer Science Cryptographic Hardware and Embedded Systems – CHES 2016*. 412-431. DOI: 10.1007/978-3-662-53140-2_20.

[27] Dhumane, A., Prasad, R., Prasad, J. (2016). Routing issues in Smart Devices: A survey. *In Proceedings of the International Multiconference of Engineers and Computer Scientists, Hong Kong*. 1:13-20.

[28] Dybå, T., Dingsøyr, T. (2008). Empirical studies of Agile Software Development: A systematic review. *Information and Software Technology*. 50(9-10):833-859. DOI:10.1016/j.infsof.2008.01.006

[29] Grobauer, B., Walloschek, T., Stöcker, E. (2013). Understanding Cloud Computing Vulnerabilities. *IEEE Security and Privacy*. 9:50-57. DOI: 10.1109/MSP.2010.115.

[30] Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. (2013). Smart Devices: A vision, architectural elements, and future directions. *Future Generation Computer System*. 29:1645-1660. DOI:10.1016/j.future.2013.01.010

[31] Hameed, S., Khan, F. I., Hameed, B. (2019). Understanding security requirements and challenges in Smart Devices: A review. *Journal Computer Network Communication*. 11:1-14. DOI:10.1155/2019/9629381

[32] Hammi, M. T., Livolant, E., Bellot, P., Serhrouchni, A., Minet, P. (2017). A Lightweight Mutual Authentication Protocol for the Smart Devices. *In International Conference on Mobile and Wireless Technology*. 3-12. *Singapore: Springer.*

[33] Harnik, D., Pinkas, B., Shulman-Peleg, A. (2017). Side channels in Cloud Services: Deduplication in Cloud Storage. *IEEE Security and Privacy*. 8:40-47. DOI: 10.11 09/MSP.2010.187

[34] Hasan, M., Mohan, S. (2019). Protecting actuators in Safety-Critical Smart Devices Systems from control spoofing attacks. *In Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things*. 8-14. DOI:10.1145/3338507.3358615

[35] Herder, C., Yu, M. D., Koushanfar, F., Devadas, S. (2014). Physical unclonable functions and applications: A tutorial. *In Proceedings of the IEEE*. 102(8):1126-1141. DOI:10.1109/JPROC.2014.2320516

[36] He, D., Zeadallyn, S. (2015). An analysis of RFID Authentication Schemes for Smart Devices in healthcare environment using Elliptic Curve Cryptography. *IEEE Smart Devices Journal*. 2(1):72-83. DOI:10.1109/JIOT.2014.2360121

[37] Kaaniche, N., Laurent, M. (2017). Data security and privacy preservation in Cloud Storage environments based on cryptographic mechanisms. *Computer Communications*. 111:120-141. DOI: 10.10 16/j.comcom.2017.07.006.

[38] Khammash, M., Tammam, R., Masri, A., Awad, A. (2021). Elliptic Curve Parameters Optimization for Lightweight Cryptography in Mobile-Ad-Hoc Networks. *In 2021 18th International Multi-Conference on Systems, Signals & Devices (SSD)*. 63-69. *IEEE.*

[39] Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. 33(2004):1-26. *Keele, UK: Keele University*.

[40] Køien, G. M. (2011). Reflections on trust in devices: An informal survey of human trust in an Smart Devices context. *Wireless Personal Communications*. 61(3):495-510. DOI:10.1007/s11277-011-0386-4

[41] Kothmayr, Thomas. (2013). DTLS based security and two-way authentication for The Smart Devices. *Ad Hoc Networks*. 11(8):2710-2723. DOI:10.1016/j.adhoc.2013.05.003

[42] Kumar, P. R., Raj, P. H., Jelciana, P. (2018). Exploring data security issues and solutions in Cloud Computing. *Procedia Computer Science*. 125:691-697. DOI: 10.1016/j. procs.2017.12.089

[43] Lai, C., Li, H., Lu, R., Shen, X. S. (2013). A secure and efficient Group Authentication and Key Agreement Protocol for LTE Networks. *Computer Network.* 57:3492-3510. DOI:10.1016/j.comnet.2013.08.003

[44] Lara-Nino, C. A., Diaz-Perez, A., Morales-Sandoval, M. (2018). Elliptic curve lightweight cryptography: A survey. *IEEE Access*. 6:72514-72550. DOI: 10.1109/ACCESS.2018.2881444

[45] Lee, J. Y. (2017). A lightweight authentication protocol for Smart Devices. *In International Symposium on Next-Generation Electronics, Kwei-Shan.*

[46] Li, F., Lai, A., Ddl, D. (2013). Evidence of Advanced Persistent Threat: A case study of malware for Political Espionage. Malicious and Unwanted Software (MALWARE). *2013 6th International Conference on IEEE*. 102-109. DOI:10.1109/MALWARE.2011.6112333

[47] Li, N., Liu, D., Nepal, S. (2017). Lightweight Mutual Authentication for Smart Devices and its applications. *IEEE Transactions on Sustainable Computing*. 2(4):359-370. DOI: 10.1109/TSUSC.2017.2716953

[48] Li, Y., Gao, M., Yang, L., Zhang, C., Zhang, B., Zhao, X. (2020). Design of and research on Industrial Measuring Devices based on Smart Devices technology. *Ad Hoc Networks*. 102:102072.

[49] Liu, C., Ranjan, R., Yang, C., Zhang, X., Wang, L., Chen, J. (2015). Top-down levelled multi-replica Merkle Hash Tree based secure public auditing for dynamic big data storage on Cloud. *IEEE Transactions on Computers*. 64:2609-2622. DOI: 10.1109/ TC.2014.2375190

[50] Liu, X., Zhao, M., Li, S., Zhang, F., Trappe. (2017). W. A security framework for the Smart Devices in the future Internet architecture. *Future Internet*. 9(3):1-27. DOI:10.3390/fi9030027

[51] Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I. (2016) Smart Devices: Vision, applications and research challenges. *Ad Hoc Networks*. 10(7):1497-1516. DOI:10.1016/j.adhoc.2012.02.016

[52] Mohsen, N. A., Jha, N. K. (2016). A comprehensive study of security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing*. 5:586-602. DOI:10.1109/TETC.2016.2606384

[53] Nicanfar, H., Jokar, P., Beznosov, K., Leung, V. C. M. (2014). Efficient authentication and key management mechanisms for smart grid communications. *IEEE System Journal*. 8:629-640. DOI:10.1109/JSYST.2013.2260942

[54] Pal, S., Hitchens, M., Varadharajan, V. (2018). Modeling identity for the Smart Devices: Survey, classification and trends. *In Proceedings of the 2018 12th International Conference on Sensing Technology (ICST), Limerick, Ireland*. 45-51. DOI:10.1109/ICSensT.2018.8603595

[55] Rashid, F., Miri, A., Woungang, I. (2012). A secure data deduplication framework for Cloud environments. *In Proceedings of the 2012 Tenth Annual International Conference on Privacy, Security and Trust, Paris, France*. 81-87. DOI: 10.1109/ PST.2012.6297923

[56] Roman, R., Zhou, J., Lopez, J. (2013). On the features and challenges of security and privacy in distributed Smart Devices. *Computer Networks*. 57(10):2266-2279. DOI:10.1016/j.comnet.2012.12.018

[57] Salleh, N., Mendes, E., Grundy, J. (2013). The effects of openness to experience on pair programming in a Higher Education context. *In 2013 24th IEEE-CS Conference on Software Engineering Education and Training (CSEE&T)*. 149-158. DOI:10.1109/CSEET.2011.5876082

[58] Schmitt, C., Noack, M., Stiller, B., Tiny, T. O. (2016). Two-way authentication for constrained devices in the Smart Devices. *In Smart Devices. Amsterdam, The Netherlands: Elsevier*. 239-258.

[59] Shahbodin, F., Azni, A. H., Ali, T., Mohd, C. K. N. C. K. (2019, January). Lightweight cryptography techniques for MHealth cybersecurity. *In Proceedings of the 2019 Asia Pacific Information Technology Conference*. 44-50. DOI:10.1145/3314527.3314536

[60] Sharma, V., Kim, J., Kwon, S., You, I., Lee, K., Yim. K. (2018). A framework for Mitigating Zero-Day Attacks in Smart Devices. *arXiv 2018*. arXiv: 1804.05549

[61] Shen, J., Yang, H., Wang, A., Zhou, T., Wang, C. (2019). Lightweight Authentication and Matrix-Based Key Agreement Scheme for Healthcare in Fog Computing. *Peer-to-Peer Network Application*. 12(4):924-933. DOI:10.1007/s12083-018-0696-3

[62] Sicari, S., Rizzardi, A., Grieco, L. A. (2015). A security, privacy and trust in Smart Devices: The road ahead. *Computer Network*. 76:146-164. DOI:10.1016/j.comnet.2014.11.008

[63] Singh, A., Chatterjee, K. (2015). A Secure Multi-Tier Authentication Scheme in Cloud Computing Environment. In Proceedings of the 2015 International Conference on Circuits. *Power and Computing Technologies [ICCPCT-2015], Nagercoil, India*. DOI:10.1109/ICCPCT.2015.7159276

[64] Singh, S., Sharma, P. K., Moon, S. Y., Park, J. H. (2017). Advanced lightweight encryption algorithms for Smart Devices devices: Survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*. 15(2):1-18. DOI:10.1007/s12652-017-0494-4

[65] Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., Choo, K. K. R. (2020). A systematic literature review of Blockchain Cyber Security. *Digital Communications and Networks*. 6(2):147-156. DOI:10.1016/j.dcan.2019.01.005

[66] Turkanovi, M. (2014). A Novel User Authentication and Key Agreement Scheme for Heterogeneous Ad Hoc Wireless Sensor Networks, based on the Smart Devices Notion. *Ad Hoc Networks*. 20:96-112. DOI:10.1016/j.adhoc.2014.03.009

[67] Wendt, J. B., Potkonjak, M. (2014). Hardware Obfuscation Using PUF-Based Logic. *In 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. 270-271.

[68] Williams, Patricia, A. H., Vincent. M. (2016). Always connected: The security challenges of the healthcare Smart Devices. *IEEE 3rd World Forum on Smart Devices (WF-Smart Devices)*. DOI: 10.1109/wf-Smart Devices.2016.7845455 2

[69] Wu, Z. Q. (2017). A Security Transmission Model for Smart Devices. *Chinese Journal of Computers*. 34(8):1351-1364. DOI:10.3724/SP.J.1016.2011.01351

[70] Yanling, Z. (2013). Research on Data Security Technology in Smart Devices. *Applied Mechanics and Materials*. 433-435, 1752-155.

[71] Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. A. (2019). Smart Devices Forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generations Computer System*. 92:265-275. DOI:10.1016/j.future.2018.09.058

[72] Ye, N., Zhu, Y., Wang, R. C., Malekian, R., Qiao-min, L. (2014). An efficient authentication and access control scheme for perception layer of Smart

Devices. *Applied Mathematics & Information Sciences.* 8(4):1617-1624. DOI:10.12785/amis/080416

[73] Dasari, K., & K. Sahadevaiah. (2025). Literature Review on Lightweight Authentication Algorithms in Remote Data Transfer. *International Journal of Computational and Experimental Science and Engineering,* 11(1). https://doi.org/10.22399/ijcesen.954

[74] Kosaraju Chaitanya, & Gnanasekaran Dhanabalan. (2024). Precise Node Authentication using Dynamic Session Key Set and Node Pattern Analysis for Malicious Node Detection in Wireless Sensor Networks. *International Journal of Computational and Experimental Science and Engineering,* 10(4). https://doi.org/10.22399/ijcesen.613

[75] Yu, S., Guo, S. (2016). Big data concepts, theories, and applications. *Cham, Switzerland: Springer International Publishing*. 1-437. DOI: 10.1007/978-3-319-27763-9