International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Review Paper

Symmetric and Asymmetric Encryption Schemes for Internet of Things: A Survey

Nusrat H. Shah*[1], Durdana T. Khan[2], Arshia A. Banu,[3] Lubna H. Shah[4]

Submitted: 28/10/2022 **Revised:** 14/12/2022 **Accepted**: 03/01/2023

Abstract*:* IoT applications such as smart homes can monitor and control users' household chores anytime and anywhere. Similarly, Body Area Networks (BANs) can monitor the physical condition of a patient via various wearable sensors. Several authentication protocols have been proposed for embedded devices based on hash chains, symmetric cryptography, or PKC (public-key cryptography). Nevertheless, approaches based on hash chains and symmetric cryptography require storing large amounts of data regarding user identities and equivalent symmetric ECC keys with an increase in the number of devices. More seriously, updating a user's key and establishing a session key in such a protocol is a complex task. The various key authentication protocol for internet of things are reviewed in this paper. The major techniques which are already been proposed are focused on the complexity of the authentication model.

Keywords: Internet of Things, Authentication, PKC, ECC

1. Introduction

The Internet of Things (IoT) represents a new development of the classic Internet network in the context of range, dimension and applications. This innovative networking platform magnifies the Cyberspace from a M2M (machine-to-machine) communication channel to a T2M (Things-to-Machine) and T2T (Things-to-Things) channel of communication. In simple terms, the goal of IoT is to turn everything into a computer that can compute and communicate over a network. IoT applications such as smart homes can monitor and control users' household chores anytime and anywhere [1]. Similarly, Body Area Networks (BANs) can monitor the physical condition of a patient via various wearable sensors. The key components of IoT applications include sensors, fixed microprocessors, IoT gateways to transfer heterogeneous network data, and a server to store, analyse and decision-making. Security challenges of IoT applications like weak passwords, plain text transmission of sensitive data, etc., have turned into very serious issues. People have become aware of the security weakness of IoT devices. Since most IoT devices are inexpensive, they have typically limited number of resources in the context of processing capacity and storage, which lead to complex cryptographic primitives and protocols taking longer to run. A standard IoT device consists of an 8- or 16-bit low-power microprocessor with an operating frequency of below 10MHz and is embedded with a few kilobytes (KB) of RAM and flash memory. It is therefore more important for IoT devices to use competent cryptographic primitives and to design light-weight protocols.

1.1. Need of Authentication in IoT

The purpose of the authentication protocol for IoT devices is to protect the identity of the devices. The server can recognize genuine or registered IoT devices, and reject illicit, unregistered or counterfeit devices. At that point, the server and the IoT device generates the session key to keep communication protected including transporting sensitive data and commands, and update the device information [2], certificates, software or firmware, among others. Therefore, the role of authentication becomes very crucial in meeting the security requirements for IoT mechanisms. In current years, several authentication protocols have been proposed for embedded devices based on hash chains, symmetric cryptography, or PKC (public-key cryptography). Nevertheless, approaches based on hash chains and symmetric cryptography require storing large amounts of data regarding user identities and equivalent symmetric keys with an increase in the number of devices. More seriously, updating a user's key and establishing a session key in such a protocol is a complex task [3]. Schemes with public-key cryptography can more efficiently address all of these challenges. But some of them require much more time to run since the public-key cryptographic algorithms used in the schemes can lead to substantial overheads with respect to time and energy exhaustion. As a competent public-key

1,2,3 Department of Computer Science and Information Technology, Jazan University, KSA
4CBA, Jazan University, KSA
ORCID ID : 0000-0003-2614-7644
** Corresponding Author Email: snusrat01@gmail.com (ORCID ID : 0000-0002-1022-4150)*

cryptographic approach that can be implemented on IoT devices, elliptic curve cryptography (ECC) has a small key size and storage than and limited computations than other public-key primitives such as Rivest Shamir Adleman (RSA), pairing and Learning with Errors (LWE) under the same protected level [4]. The level of security provided by a 160-bit ECC key is the same as that of a 1024-bit RSA key. The calculated cost of coupling is about 20 times more than that of scalar multiplication at the same protection level. The benefits offered by ECC can be significant in scenarios with constrained processing power, storage, bandwidth or energy expenditure. With regard to authentication challenges in IoT applications, some researchers have also proposed relevant security solutions.

1.2. Elliptic Curve Cryptography (ECC)

In the mid-1980s, Victor Miller and Neil Koblitz were the first to independently use elliptic curves for cryptography. Elliptic curve cryptography calculations are built on finite fields, which can choose to be either a prime region or a binary region [5]. Elliptic Curve Cryptography (ECC) uses an elliptic curve defined over a finite field$\mathbb{F}_q$,which is represented by $E(\mathbb{F}_q)$and consists of affine points $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$to satisfy the Weierstrass equation (1).

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, where\ a_i \in \mathbb{F}_q$$

i. $E(\mathbb{F}_q)$ with a particular point form an abelian group called the point at infinity $\mathcal{O}$. The $\mathcal{O}$ group acts as a neutral element in the operation. The security of ECC lies on the complexity of providing solution to the Discrete Logarithm Problem on such a group, shortened as ECDLP, for which only ii. algorithms with exponential computational difficulties are recognized. Properties that make solving ECDLP difficult. It is quite hard to locate a group $E(\mathbb{F}_q)$with the desired features that make it difficult to solve ECDLP. Therefore, elliptic curves considered safe are reported in the literature and included in the standards. Traditional PKC based on ECC generally uses these standardized structures, which outline the safe recognition of ECC, but were not considered to be used in controlled situations. In current years, the definition of new elliptic [6] curves tries to obtain higher security level but with lower operating costs and a smaller number of hardware resources needed to perform computing competently. These are outside the scope of the new elliptical curve standards but are an attractive alternative to iii. WSN, RFID, e-health and other emerging technologies in the IoT domain.

1.3. Review of Existing Authentication Protocols

Debiao et al.'s ID-based remote user authentication scheme, and Goutham et al.'s scheme (which is a modified version based on previous one) are the two most common ECC based authentication schemes for low resource devices. These protocols have three fundamental phases. 1) system initialization phase, 2) client registration phase. 3) mutual authentication with key agreement phase. The Goutham et al.'s scheme includes two more phases known as max, min values and USN phase and identity updating phase [7].

A. Debiao et al.'s scheme

1. System Initialization Phase: In this phase, server S produces system parameters in the following way: Sselects an elliptic curve equation Eover a finite field$\mathbb{F}_p$, and a base point $P \in E(\mathbb{F}_p)$ of order n. At this point,Schooses its master key $x$and calculates equivalent public key $P_s = xP$. Along with achieve initialization, Salso requires some auxiliary calculation modules like three secure one-way hash function H_1, H_2, H_3 and a message authentication code $MAC_k(m)$. Then, S maintains master key $x$as a secret, and publishes system parameter tuple$\left(\mathbb{F}_p, E, n, P, P_s, H_1, H_2, H_3, MAC_k(m)\right)$.

2. Client registration phase: When a client $C_i$wishes to register to the server S, $C_i$submits its identity $IDC_i$to S. Scomputes $h_{C_i} = H_1(IDC_i)$ by IDC_i and H_1, client's private key $DC_i = \frac{1}{x+h_{C_i}}P \in G$, then S sends $DC_i$to $C_i$through a secure channel. The corresponding public key is $P_{C_i} = (h_{C_i} + x)P = h_{C_i}P + P_s$[8].

3. Mutual authentication with key agreement phase: In this phase, the client $C_i$requests server Sthrough a message

Client $C_i$chooses a random number $r_{C_i} \in Z_n^*$, and computes $M = r_{C_i}.P, M' = r_{C_i} \cdot D_{C_i}$, $k = H_2(ID_{C_i}, T_{C_i}, M, M')$, where $T_{C_i}$is the current timestamp of client. Then, $C_i$sends the request message $M_1 = \{ID_{C_i}, T_{C_i}, M, M\ AC_k(ID_{C_i}, T_{C_i}, M)\}$to the server.

After receiving M_1, Schecks the validity of $ID_{C_i}$and the time freshness of T_{C_i}firstly. The freshness is decided by$T' - T_{C_i} < \Delta T$, T' is current time of server and $\Delta T$is the valid time interval. Scontinues the execution only if time verification passes. S computes$h_{C_i} = H_1(IDC_i)$, $M' = \frac{1}{x+h_{C_i}}M$and $k = H_2(IDC_i, TC_i, M, M')$, and then uses$k$ to check the integrity of $M\ AC_k(ID_{C_i}, T_{C_i}, M)$ [9].Swill quit the current session if the check produces a negative result. Otherwise, S chooses a random number$r_s \in Z_n^*$ and computes $W = r_s \cdot P, K = r_s \cdot M$and the session key $sk = H_3(IDC_i, TC_i, T_s, M, W, K_s)$.Then Ssends $M_2 = \{IDC_i, T_s, W, M\ AC_k(ID_{C_i}, T_s, W)\}$ to C_i,where $T_s$is server's current timestamp.

Upon receiving M_2, $C_i$checks the integrity of $M\ AC_k(ID_{C_i}, T_s, W)$using key k, and then $C_i$computes $K_{C_i} = r_{C_i} \cdot W$and computes the session key $sk = H_3(IDC_i, TC_i, T_s, M, W, K_{c_i})$.

B. Goutham et al.'s scheme

The scheme of Goutham et al.is an improved version of the earlier scheme, which includes some new secure features such as anonymous, identity updating in the protocol. overall, the step of Goutham's is similar to the step of

Debiao et al.'s, and the different processes are pointed out below:

1. Max, Min values and USN phase: The Max, Min value and USNphase is before user registration phase, and it helps user to hide its identity. These three values are assigned by server. The anonymous ID chosen by the user is between Min and Max. The USN value that helps server to find user's information in database is a unique sequence number of user. Max, Min and USNvalues are saved in server-side [10].

2. The Anonymous Process: In order to achieve user identity anonymity, $USN$is assigned to represent the unique user identity, and server could search$USN$to find user's Max and Minvalues. At last, the original identity is computed by anonymous identity, Min and Maxvalues. The anonymity process runs at the beginning of mutual authentication with key agreement phase as follows.

i. Client C_i computes its anonymous ID by performing $U_R = Rand\%(Max = Min + 1) + Max, AID_U = ID_U \oplus H_2(U_R \parallel T_U)$,

ii. Client $C_i$sends M_1 to S, which is similar to the previous scheme, except usingAIDinstead of $ID$and inserting 2 parameters $USN$and $Rand. M_1 = \{AID_{C_i}, TC_i, R = r_u \cdot P, USN, Rand, M\ AC_k(ID_{C_i}, T_{C_i}, R)\}$.

iii. Server Sneeds to remove anonymous firstly when it receives $M_1$by identifying USNvalue, then computes C_i's real ID using the corresponding Min and Max. $U_R = Rand\%(Max = Min + 1)$. Finally, Scontinues mutual authentication process as Debiao's [11].

3. Identity Updating Phase: Client $C_i$can launch identity updating phase when it wants to change its original identity ID_{C_i}. The phase above can prevent parts of malicious attack from adversary:

i. Client $C_i$re-selects an identity $ID_{C_i}^{\#}$and computes$AID_{C_i} \oplus ID_{C_i}^{\#}$and sends Sa request message $M = \{AID_{C_i}, AID_{C_i}^{\#}, USN, Rand, TC_i, M\ AC_k(ID_{C_i}, ID_{C_i}^{\#})\}$.

ii. Server Sreceives the re-selected ID_{C_i} as $ID_{C_i}^{\#} = ID_{C_i} \oplus AID_{C_i}^{\#}$,and then Server Supdates $ID_{C_i}^{\#}$and computes $h_{C_i}^{\#} = H_1(ID_{C_i}^{\#})$and client's secret key $x_{C_i}^{\#} = \frac{1}{qs.h_{C_i}} \cdot P$,and then delivers a message $\{x_{C_i}^{\#}, Max, Min, USN\}$to the client smart card through a secure channel or an off-line interaction [12].

2. Literature Review

2.1 Elliptic Curve Cryptographic (ECC) based Lightweight Authentication Protocol.

Aakanksha Tewari, et.al (2018) introduced an ECC (Elliptic Curve Cryptographic) based lightweight authentication protocol for IoT (Internet of Things) devices in which RFID (Radio Frequency Identification) tags were implemented at the physical layer [13]. The ECC provided more stability and security to this protocol utilizing few resources in comparison with other methods. An analysis was conducted for computing the introduced protocol with regard to security. The results demonstrated that the introduced protocol offered mutual authentication and kept the data confidential. Manasha Saqib, et.al (2021) developed a 3-factor authentication model for significant applications of IoT (Internet of Things) which were planned on the basis of identity, password and a digital signature method [14].

A publish subscribe pattern was implemented in which ECC (elliptical curve cryptography) and computationally low hash chains were employed. This model offered resistance against diverse kinds of cryptographic attacks. Scyther tool was utilized to validate the developed model. The results exhibited that the developed model was efficient for saving the band width and communication energy and alleviated computing and communicating costs of sensor nodes consisted of limited resources. Vidya Rao, et.al (2020) projected a hybrid authentication and data integrity technique in which digital signature and encryption method was deployed based on ECC (elliptic curve cryptography) [15]. Raspberry Pi-3 was utilized to conduct the experimentation. The results of experiments confirmed that the projected technique enhanced the time up to 33.3% during the signature stage and 15.6 % during the authentication stage as compared to the traditional techniques. Utkalika Satapathy, et.al (2018) established a lightweight authentication technique on the basis of ECC (Elliptic Curve Cryptographic) to attain satisfactory security measures and higher efficacy [16]. This technique was adopted for authenticating the device and to monitor a smart home and the home server gateway that was considered as a major point for all IoT devices whose implementation was done in the home. The experimental results validated that the established technique performed accurately in logical way and offered superior level with the help of BAN (Burrows-Abadi-Needham) logic. Sahil Garg, et.al (2020) presented a lightweight authentication and key agreement protocol for the IoT environment on the basis of a hierarchical approach which offered robustness and security [17]. This protocol was depending upon lightweight operations namely EEC (elliptic curve cryptography), hash functions and XOR operations. Afterward, the AVISPA (automated validation of Internet security protocols and applications) was applied for quantifying the presented protocol. The results confirmed that the presented protocol mutually authenticated the IoT (Internet of Things) nodes with server and provided resistance against several attacks. Moreover, the cost of this protocol was lower in contrast to other protocols.

2.1 Table of Comparison

Author	Year	Technique Used	Advantages	Disadvantages
Aakanksha Tewari, et.al	2018	ECC (Elliptic Curve Cryptographic) based lightweight authentication	The introduced protocol offered mutual authentication and kept the data confidential.	The introduced protocol was not effective to secure the network from DDoS (Distributed Denial of Service) attacks and spam attacks launched on IoT devices.
Manasha Saqib, et.al	2021	Three-factor authentication model	This model was adaptable for a practical IoT-based framework due to its reliability, lightweight nature and security.	This model performed poorly on sophisticated platforms.
Vidya Rao, et.al	2020	A hybrid authentication and data integrity method	The projected technique enhanced the time up to 33.3% during the signature stage and 15.6% during the authentication stage.	The projected technique provided lower efficacy in case of diverse kinds of large-scale applications.
Utkalika Satapathy, et.al	2018	A lightweight authentication scheme based on ECC	The established technique performed accurately in logical way and offered superior level with the help of BAN logic.	The issues were occurred when the established technique was scaled on a real environment.
Sahil Garg, et.al	2020	Lightweight and secure authentication and key agreement protocol	The presented protocol mutually authenticated the IoT (Internet of Things) nodes with server and provided resistance against several attacks.	The protocol utilized a centralized server for authentication on IoT nodes.

2.2 Authentication Protocol for Resource Constricted Devices

Sarmadullah Khan, et.al (2019) suggested a resource-effective security method in which the devices were authenticated with their network managers, authentication among devices on different networks, and the process to establish an attack-resilient key were comprised [18]. The suggested method was evaluated by analyzing various attack scenarios. The experimental results depicted that the suggested method was able to utilize least memory in the authentication and consume lower power while producing a key. In addition, this method was assisted in protecting the network from diverse attacks. Xuyang Ding, et.al (2021) designed a lightweight anonymous authentication technique for low resource devices in IoT (Internet of Things) [19]. The designed technique was applicable for deploying anonymous authentication and protecting privacy on an insecure channel and fulfilling some security factors including unsinkability and forward secrecy. The experimental outcomes revealed that the designed technique was capable of mitigating the computational cost and communication cost and ensured the security. Thus, the adaptability of the designed technique was proved for resource constrained devices of IoT. Chau D. M. Pham, et.al (2021) recommended a mutual authentication protocol to preserve privacy on the basis of ECC (Elliptic Curve Cryptographic) so that resources were utilized efficiently and the privacy of involved devices was preserved [20]. The traditional protocol was expanded to develop this protocol. BAN (Burrows-Abadi-Needham) logic was applied to compute the accuracy of the recommended protocol. The informal analysis represented the resiliency of this protocol against various attacks. The D2D (device to device) authentication stage led to attain superior energy usage as compared to the existing techniques. The results proved the applicability and security of the recommended protocol for small devices which consisted of limited. Syed Wajid Ali Shah, et.al (2020) projected a new and lightweight CA (Continuous Authentication) protocol in which communication channel properties and a tunable mathematical function were deployed for creating the session keys which were changed in dynamic way [21]. This protocol offered resistance against attack vectors. This protocol was adaptable to secured2d (device to device) communication which was crucial and contained limited resources.

Bahaa Hussein Taher, et.al (2019) established a lightweight authentication protocol having robustness and security to deal with the limitations of IoT devices containing low resources [22]. The information related to the biometrics of user was handled using fuzzy extraction and a level 3 feature extractor. The established protocol was evaluated on BAN (Burrows-Abadi-Needham) logic. The results indicated that the established protocol had resistance against diverse malicious attacks and applicability for various applications in IoT environment in comparison with other protocols.

2.2 Table of Comparison

Author	Year	Technique Used	Advantages	Disadvantages
Sarmadullah Khan, et.al	2019	A resource-effective security method	The suggested method was able to utilize least memory in the authentication and consume lower power while producing a key.	This technique performed ineffectively for other cyber security protocols, such as IPsec/IKE.
Xuyang Ding, et.al	2021	A lightweight anonymous authentication technique	The designed technique was capable of mitigating the computational cost and communication cost and ensured the security.	This technique was incapable of covering the devices based on the Telosb platform
Chau D. M. Pham, et.al	2021	Mutual privacy-preserving authentication protocol	The D2D (device to device) authentication stage of this protocol led to attain superior energy usage as compared to the existing techniques.	This protocol had not protected the privacy in some scenarios due to which lower security was obtained.
Syed Wajid Ali Shah, et.al	2020	Lightweight and secure CA () protocol	This protocol was adaptable to secured2d (device to device) communication which was crucial and contained limited resources.	This protocol yielded lower efficiency in some security scenarios.
Bahaa Hussein Taher, et.al	2019	Lightweight, robust and secure authentication protocol	The established protocol was proved secure and attained more efficiency concerning computing and communicating costs.	This technique provided poor performance on large-scale applications.

2.3 Lightweight PUF-Based Authentication Protocol

Fadi Farha, et.al (2021) intended a lightweight SRAM (static random access memory)-authentication method based on PUF (Physical Unclonable Functions) for ensuring the reliability of the accessed end devices [23]. The reordered memory displayed CRPs (challenge-response pairs) whose deployment was done in this method as challenges and startup values of the corresponding SRAM cells as responses. The experimental results validated the effectiveness of the intended method for authenticating IoT devices with constricted resources and attained lower computation overhead and least memory capacity. Tarek A. Idriss, et.al (2021) formulated aLPA (lightweight PUF-based authentication) protocol in which process of recognizing secret pattern was executed to offer mutual authentication and to exchange genuine secret message for constrained devices on (Internet of Things) [24]. This protocol made the implementation of any effective PUF (Physical Unclonable Functions) circuit to construct a soft

model. The results exhibited that the formulated protocol was resilient to modeling attacks. Karim Lounis, et.al (2019) introduced a new lightweight T2T-MAP (mutual authentication protocol) for which PUFs (Physical Unclonable Functions) were exploited [25]. This protocol assisted every device in uniquely recognizing and authenticating itself in an IoT infrastructure. The security of this protocol was computed in a security analysis for tackling known attacks. The resource-constrained devices were applied to deploy this protocol and analyze it. The results depicted that the introduced protocol was authentic and offered adequate overhead and least energy utilization. HüsnüYıldız, et.al (2021) designed a PLGAKD (PUF-based lightweight group authentication and key distribution) protocol for removing attacks and network issues [26]. PUF (Physical Unclonable Function) was utilized to authenticate a group and distribute a key. The factorial tree and CRT was implemented for lessening the communication as well as storage overhead. The designed protocol had potential to mitigate the overhead for different secrecy in comparison with other protocols. Konstantinos Goutsos, et.al (2019) presented a pair-wise CA (continuous authentication) protocol on the basis of PUFs (Physical Unclonable Functions) and provided mutual authentication to nodes containing constricted resources [27]. The presented protocol was secure in IoT applications in which numerous devices were comprised. This technique provided lower computation cost and energy utilization.

2.3 Table of Comparison

Author	Year	Technique Used	Advantage	Disadvantage
Aakanksha Tewari, et.al	2018	ECC (Elliptic Curve Cryptographic) based lightweight authentication	The introduced protocol offered mutual authentication and kept the data confidential.	The introduced protocol was not effective to secure the network from DDoS (Distributed Denial of Service) attacks and spam attacks launched on IoT devices.
Manasha Saqib, et.al	2021	Three-factor authentication model	This model was adaptable for a practical IoT-based framework due to its reliability, lightweight nature and security.	This model performed poorly on sophisticated platforms.
Vidya Rao, et.al	2020	A hybrid authentication and data integrity method	The projected technique enhanced the time up to 33.3% during the signature stage and 15.6% during the authentication stage.	The projected technique provided lower efficacy in case of diverse kinds of large-scale applications.
Utkalika Satapathy, et.al	2018	A lightweight authentication scheme based on ECC	The established technique performed accurately in logical way and offered superior level with the help of BAN logic.	The issues were occurred when the established technique was scaled on a real environment.
Sahil Garg, et.al	2020	Lightweight and secure authentication and key agreement protocol	The presented protocol mutually authenticated the IoT (Internet of Things) nodes with server and provided resistance against several attacks.	The protocol utilized a centralized server for authentication on IoT nodes.

3. Major Findings

This section presents the state-of-the-art review layout, a step-by-step method for the literature discussed in the previous sections. This research focuses on categorizing the current literature on authentication protocols assessing the current trends. This evaluation finds relevant research articles from reputable electronic databases and the top conferences in the field. After then, inclusion and exclusion criteria were used to reduce the number of papers that were considered. Following that, final research studies were chosen based on a variety of variables. The information given here is the product of a thorough investigation. For this review study, various electronic database sources were investigated; some of the popular electronic databases used in this search like google scholar, Elsevier, Science direct etc. Using the inclusion criterion, which mainly depends on the techniques, the relevant work of security algorithms is retrieved from the enormous collection of data given by search engines. The data shows that journals account for most of the work in this study (51%), with conferences accounting for 40% of the work and book chapters accounting for 9%. In addition, the data depicts a year-by-year's study of work relevant to authentication protocols of IOT. The major data is available on the google scholar as compared to Elsevier and Science direct. The google scholar has 60 percent data, Elsevier has approx. 10 percent and Science direct has approx. 30 data on authentication protocols. The data division has been presented in figure 1.

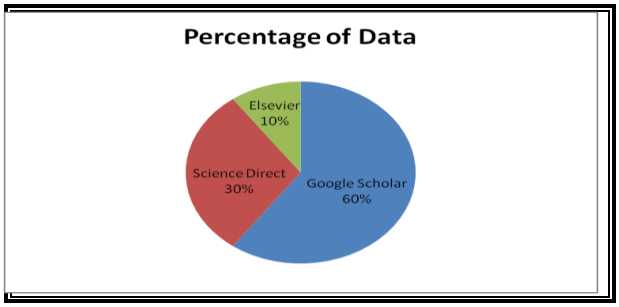

Fig 1: Percentage of Data Sharing

In Figure 1, the percentage of data sharing is shown in figure approx. 60 percent data is available on Google scholar, 30 percent is available on science direct and very less amount of data that is 10 percent is available on Elsevier.

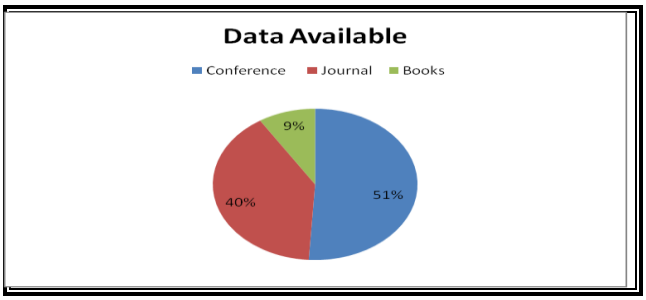

Fig 2: Data Available

As shown in figure 2, the data is available through conferences, journals and books. The conferences have approx. 51 percent of total data, 40 percent data is available through journals and 9 percent is available through books.

4. Conclusion

Several authentication protocols have been proposed for embedded devices in IoT based on hash chains, symmetric cryptography, or PKC (public-key cryptography). Nevertheless, approaches based on hash chains and symmetric cryptography require storing large amounts of

data regarding user identities and equivalent symmetric keys with an increase in the number of devices. It is analyzed that all the Scopus indexed journals have published papers and approx. 51 percent are published in the conferences. The major content related to lightweight protocols are available on the google scholars. It is analyzed from the results that in the major protocols complexity is reduced for the authentication.

References

[1] N. Druml et al., "A Flexible and Lightweight ECC-Based Authentication Solution for Resource Constrained Systems," 2014 17th Euromicro Conference on Digital System Design, 2014, pp. 372-378

[2] S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed, F. Gagnon and M. Guizani, "ECC-based Secure and Lightweight Authentication Protocol for Mobile Environment," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2019, pp. 1-6

[3] S. Khan and R. K. Aggarwal, "Efficient Mutual Authentication mechanism to Secure Internet of Things (IoT)," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), 2019, pp. 409-412

[4] S. Shamshad, K. Mahmood, S. Kumari and M. K. Khan, "Comments on "Insider Attack Protection: Lightweight Password-Based Authentication Techniques Using ECC"," in IEEE Systems Journal, vol. 15, no. 1, pp. 877-880, March 2021

[5] U. Satapathy, B. K. Mohanta, D. Jena and S. Sobhanayak, "An ECC based Lightweight Authentication Protocol For Mobile Phone in Smart Home," 2018 IEEE 13th International Conference on Industrial and Information Systems (ICIIS), 2018, pp. 303-308

[6] E. Lara, L. Aguilar and J. A. García, "Lightweight Authentication Protocol Using Self-Certified Public Keys for Wireless Body Area Networks in Health-Care Applications," in IEEE Access, vol. 9, pp. 79196-79213, 2021

A. B. AMOR, M. ABID and A. MEDDEB, "SAMAFog: Service-Aware Mutual Authentication Fog-based Protocol," 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), 2019, pp. 1049-1054

[7] G. Shen and B. Liu, "Research on Embedding ECC into RFID Authentication Protocol," 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012, pp. 1835-1838

[8] M. K. Gupta, R. Kumar and S. Kumari, "Flaws and Amendment in an ECC-based Authentication Scheme for SIP," 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), 2020, pp. 372-376

[9] S. Garg, K. Kaur, G. Kaddoum and M. Client, "ECC-based Secure and Provable Authentication Mechanism for Smart Healthcare Ecosystem," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 2020, pp. 1-6

[10] H. Debiao, C. Jianhua, and H. Jin, "An id-based client authentication with key agreement protocol for mobile client–server environment on ecc with provable security," Information Fusion, vol. 13, no. 3, pp. 223–230, 2012.

[11] R. A. Goutham, G.-J. Lee, and K.-Y. Yoo, "An anonymous id-based remote mutual authentication with key agreement protocol on ecc using smart cards," in Proceedings of the 30th Annual ACM Symposium on Applied Computing. ACM, 2015, pp. 169–174.

[12] Aakanksha Tewari, B. B. Gupta, "A robust anonymity preserving authentication protocol for IoT devices", 2018, IEEE International Conference on Consumer Electronics (ICCE)

[13] Manasha Saqib, Bhat Jasra, Ayaz Hassan Moon, "A lightweight three factor authentication framework for IoT based critical applications", 2021, Journal of King Saud University - Computer and Information Sciences

[14] Vidya Rao, Prema K. V., "Lightweight Authentication and Data Encryption Scheme for IoT Applications", 2020, IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)

[15] UtkalikaSatapathy, Bhabendu Kumar Mohanta, Debsish Jena, SrichandanSobhanayak, "An ECC based Lightweight Authentication ProtocolFor Mobile Phone in Smart Home", 2018, IEEE 13th International Conference on Industrial and Information Systems (ICIIS)

[16] Sahil Garg, Kuljeet Kaur, Georges Kaddoum, Kim-Kwang Raymond Choo, "Toward Secure and Provable Authentication for Internet of Things: Realizing Industry 4.0", 2020, IEEE Internet of Things Journal

[17] Sarmadullah Khan, Ahmed Ibrahim Alzahrani, Osama Alfarraj, Nasser Alalwan, Ali H. Al-Bayatti, "Resource Efficient Authentication and Session Key Establishment Procedure for Low-Resource IoT Devices", 2019, IEEE Access

[18] Xuyang Ding, Xiaoxiang Wang, Ying Xie, Fagen Li, "A Lightweight Anonymous Authentication Protocol for Resource-Constrained Devices in Internet of Things", 2021, IEEE Internet of Things Journal

[19] Chau D. M. Pham, Tran Khanh Dang, "A lightweight authentication protocol for D2D-enabled IoT systems with privacy", 2021, Pervasive and Mobile Computing

[20] Syed Wajid Ali Shah, Naeem Firdous Syed, ArashShaghaghi, Adnan Anwar, Zubair Baig, Robin Doss, "Towards a Lightweight Continuous

Authentication Protocol for Device-to-Device Communication", 2020, IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)

[21] Bahaa Hussein Taher, Sheng Jiang, Ali A. Yassin, Hongwei Lu, "Low-Overhead Remote User Authentication Protocol for IoT Based on a Fuzzy Extractor and Feature Extraction", 2019, IEEE Access

[22] Fadi Farha, Huansheng Ning, Karim Ali, Liming Chen, Christopher Nugent, "SRAM-PUF-Based Entities Authentication Scheme for Resource-Constrained IoT Devices", 2021, IEEE Internet of Things Journal

[23] Tarek A. Idriss, Haytham A. Idriss, Magdy A. Bayoumi, "A Lightweight PUF-Based Authentication Protocol Using Secret Pattern Recognition for Constrained IoT Devices", 2021, IEEE Access

[24] Karim Lounis, Mohammad Zulkernine, "T2T-MAP: A PUF-Based Thing-to-Thing Mutual Authentication Protocol for IoT", 2019, IEEE Access

[25] HüsnüYıldız, Murat Cenk, ErtanOnur, "PLGAKD: A PUF-Based Lightweight Group Authentication and Key Distribution Protocol", 2021, IEEE Internet of Things Journal

[26] Konstantinos Goutsos, Alex Bystrov, "Lightweight PUF-based Continuous Authentication Protocol", 2019, International Conference on Computing, Electronics & Communications Engineering (iCCECE)